



| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |

NASA Procedural Requirements

NPR 1600.2A

Effective Date: September 11,
2019

Expiration Date: September 11,
2024

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

NASA Classified National Security Information (CNSI)

Responsible Office: Office of Protective Services

Table of Contents

Preface

- P.1 Purpose
- P.2 Applicability
- P.3 Authority
- P.4 Applicable Documents and Forms
- P.5 Measurement/Verification
- P.6 Cancellation

Chapter 1. Introduction

- 1.1 Overview
- 1.2 Responsibilities

Chapter 2. CNSI Management

- 2.1 General
- 2.2 Original Classification
- 2.3 Classification Levels
- 2.4 NASA Original Classification Authority
- 2.5 Classification Categories
- 2.6 Application of Original Classification Authority
- 2.7 Derivative Classification
- 2.8 Application of Derivative Classification Authority
- 2.9 Identification, Designation and Markings
- 2.10 Working Papers
- 2.11 Classification Prohibitions and Limitations

- 2.12 Classification Challenges
- 2.13 Declassification Authority
- 2.14 Declassification
- 2.15 Access to CNSI
- 2.16 Accountability and Control of CNSI
- 2.17 Accountability Logs
- 2.18 Handling of Incoming Classified Material
- 2.19 Record of Destruction
- 2.20 Inventory Requirements
- 2.21 Top Secret Inventory
- 2.22 Guidelines for Electronic Classified Information Processing
- 2.23 Storage of CNSI - Security Containers and Vaults
- 2.24 Forms
- 2.25 Storage of NATO Classified Information and FGI
- 2.26 Emergency Authority
- 2.27 Reproduction of CNSI
- 2.28 Hand-Carrying and Receipting of Classified Material
- 2.29 Transmission of Classified Material
- 2.30 Receipt System
- 2.31 Defense Courier Service Reimbursement Program
- 2.32 Disposition or Destruction of Classified Material
- 2.33 Destruction Procedures
- 2.34 Sanctions
- 2.35 Security Violations, Security Infractions and Compromise of CNSI
- 2.36 CNSI Meetings
- 2.37 Security Areas
- 2.38 Classified Material Ownership
- 2.39 Security Classification Reviews for NASA Programs and Projects
- 2.40 Access to Classified National Security Information Granted by Another Government Agency
- 2.41 Special Access Program (SAP)
- 2.42 Information Systems (IS)
- 2.43 ISOO Reporting Requirements
- 2.44 Self-Inspections

Chapter 3. Sensitive Compartmented Information Programs

- 3.1 General
- 3.2 Information Systems for processing (SCI) information
- 3.3 Self-Inspections of the SCI Program
- 3.4 Facility Accreditations
- 3.5 Contractors performing SCI
- 3.6 Standard Classification Markings
- 3.7 Storage
- 3.8 SCI Accountability
- 3.9 Media
- 3.10 Document Control Procedures
- 3.11 Transportation of SCI
- 3.12 Electronic Transmissions

- 3.13 Emergency Plans
- 3.14 Request for SCI Access
- 3.15 Reporting Requirements
- 3.16 SCIF Construction Procedures
- 3.17 Co-Use Agreements
- 3.18 SCI File Transmission Procedures
- 3.19 SCI Visit Requests
- 3.20 Training

Chapter 4. Security Education and Training

- 4.1 General
- 4.2 Initial Security Education and Training
- 4.3 Annual Refresher Security Education and Training
- 4.4 Original Classification Training
- 4.5 Derivative Classifier Training
- 4.6 Other Specialized Security Education and Training
- 4.7 Termination Briefings

Chapter 5. Industrial Security

- 5.1 General
- 5.2 DoD Support
- 5.3 NISP Responsibilities
- 5.4 Suspension, Revocation, and Denial of Access to Classified Information
- 5.5 Requirements of DD Form 254

Appendix A. Definitions

Appendix B. Acronyms

Appendix C. Derivative Classification in Electronic Media

Appendix D. References

Preface

P.1 Purpose

- a. This NASA Procedural Requirement (NPR) establishes Agency-wide requirements for the protection of Classified National Security Information (CNSI).
- b. This NPR prescribes personnel responsibilities and procedural requirements for the management of CNSI to assist NASA Centers and Component Facilities in executing the NASA security program designed to protect people, property, and information.
- c. In accordance with, Classified National Security Information, Executive Order (E.O.) 13526, and 32 CFR pt. 2001, this NPR establishes Agency procedures for the proper implementation and management of a uniform system for classifying, safeguarding, and declassifying national security information generated by, for, or in the possession of NASA.

P.2 Applicability

- a. This NPR is applicable to NASA Headquarters and all NASA Centers, including Component Facilities, Technical and Service Support Centers. This language applies to the Jet Propulsion Laboratory (JPL) (a Federally Funded Research and Development Center (FFRDC)), other contractors, recipients of grants and cooperative agreements, and parties to other agreements only to the extent specified or referenced in the applicable contracts, grants, or agreements.
- b. This NPR is applicable to all NASA civil service employees, NASA contractor employees, personnel completing work through Space Act Agreements or Memorandums of Agreement (MOA) or Memorandums of Understanding (MOU), those assigned or detailed under the partners, recipients of grants and cooperative agreements, visitors, and other binding transactions in which access to Classified National Security Information is required for performance of the work.
- c. Chapter 5 is applicable to contracts, grants, cooperative agreements, and other binding transactions in which performance requires access to CNSI by the contractor, supplier, grantee, or its employees. It does not apply to agreements with other Federal agencies.
- d. In this directive, all document citations are assumed to be the latest version unless otherwise noted.
- e. In this NPR, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms: "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive materials.

P.3 Authority

- a. The National Aeronautics and Space Act, 51 United States Code (U.S.C.), Security Requirements § 20132, Dec 18, 2010.

b. Classified National Security Information, E.O. 13526, 75 Fed. Reg. 707 (Jan. 5, 2010).

P.4 Applicable Documents and Forms

a. Freedom of Information Act, 5 U.S.C. § 552

b. Privacy Act of 1974, 5 U.S.C. § 552a.

c. Intergovernmental Personnel Act, as amended, 5 U.S.C. § 3372.

d. Atomic Energy Act of 1954, 42 U.S.C. § 2011 et seq.

e. Records Management by Federal Agencies, 44 U.S.C. §§ 2905, 3101, and 3102.

f. National Security Act of 1947, 50 U.S.C. § 2671 et seq.

g. National Security Act of 1947, 50 U.S.C. § 3001 et seq.

h. National Industrial Security Program, E.O. 12829, 58 Fed. Reg. 3479 (Jan. 6, 1993).

i. Access to Classified Information, as amended, E.O. 12968, 60 Fed. Reg. 40245 (Aug. 7, 1995).

j. Information Security Program, 14 CFR pt. 1203.

k. Export Administration Regulations, 15 CFR pts. 730-774.

l. International Traffic in Arms Regulations, 22 CFR pts. 120-130.

m. Classified National Security Information, 32 CFR pt. 2001.

n. National Industrial Security Program, 32 CFR pt. 2004.

o. Federal Acquisition Regulation (FAR), 48 CFR subpt. 4.4.

p. NASA FAR Supplement (NFS), 48 CFR subpart 1804.4.

q. NASA Policy Directive (NPD) 1210.2, NASA Surveys, Audits, and Review Policy

r. NPD 1600.4, National Security Programs.

s. NPD 1600.9, NASA Insider Threat Program.

t. NPR 1441.1, NASA Records Management Program Requirements.

u. NPR 1600.3, Personnel Security.

v. NPR 1600.4, Identity and Credential Management.

w. NPR 1600.6, Communications Security (COMSEC).

x. NPR 1620.3, Physical Security Requirements for NASA Facilities and Property.

y. NPR 1660.1C, NASA Counterintelligence and Counterterrorism.

z. NPR 4100.1F, NASA Supply Support and Material Management.

aa. NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

- bb. NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements.
- cc. NPR 7120.8, NASA Research and Technology Program and Project Management Requirements.
- dd. Guidelines for Data Spillages, ITS-HBK-2820.09-04.
- ee. NASA Handbook for Writing Security Classification Guides.
- ff. NASA Form (NF) 387, Classified Material Receipt.
- gg. NF 1733, Information and Technology Classification and/or Sensitivity Level Determination Checklist.
- hh. NF 1833, Request for SCI Classified Visit.
- ii. Committee on National Security Systems (CNSS) Instruction 1253.
- jj. Federal Qualified Products List of Products Qualified Under Federal Specification FF-L-2740A Locks, Combination, Federal Specification FF-L-2740.
- kk. Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation.
- ll. Intelligence Community Directive (ICD) 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information.
- mm. Intelligence Community Directive (ICD) 705, Sensitive Compartmented Information Facilities.
- nn. ISOO Booklet, Marking Classified National Security Information.
- oo. National Industrial Security Program Operation Manual (NISPOM) DoD 5220.22-M.
- pp. National Institute of Standards and Technology (NIST) Special Publications 800-53 and 800-37.
- qq. NSA/Central Security Service Policy 9-12.
- rr. Security Executive Agent Directive 3 (SEAD 3).
- ss. Special Historical Records Review Plan (Supplement).
- tt. U. S. Security Authority for North Atlantic Treaty Organization Affairs (USSAN) Instruction 1-07.
- uu. DD Form 254, Department of Defense Contract Security Classification Specification.
- vv. SF 311, Agency Security Classification Management Program Data.
- ww. SF, 700, Security Container Information.
- xx. SF 701, Activity Security Checklist.
- yy. SF 702, Security Container Check Sheet.
- zz. SF 703, Top Secret Coversheet.

aaa. SF 704, Secret Cover Sheet.

bbb. SF 705, Confidential Cover Sheet.

ccc. SF 706, Top Secret Label.

ddd. SF 707, Secret Label.

eee. SF 708, Confidential Label.

fff. SF 710, Unclassified Label.

ggg. SF 715, Declassification Review Tab.

hhh. SF 716, Agency Security Classification Costs Estimates.

iii. Special Access Request (SAR) Form 2018a.

P.5 Measurement/Verification

a. To determine Center compliance with E.O. 13526, 32 CFR pt. 2001, and this NPR, Center Directors and Center Chiefs of Protective Services/Chief of Security (CCPS/CCS) or their designees will determine and document compliance through annual self-assessments and reviews conducted by the Office of Protective Services (OPS). Each Center Protective Services Office will conduct assessments of select organizations throughout their Center on a yearly basis to determine if Center organizations are in compliance with this NPR. OPS will provide the Centers with an OPS Self-Inspection Checklist to be used in conjunction with the NPR to ensure that all Center reviews will be tailored to include all steps necessary to perform a comprehensive review of all pertinent areas within a Center.

b. OPS will conduct evaluations, by way of the functional review process, of Center compliance and implementation. OPS will evaluate each Center at least every three years, or sooner if required, using the OPS Functional Review Checklist to determine compliance with this NPR. The functional review process will identify non-compliant issues (findings), observations, and best practices. Non-compliance with this NPR, the E.O. 13526, and/or 32 CFR pt. 2001, will result in findings that will be forwarded to the Center Director and the Assistant Administrator (AA) for Protective Services. The findings from the OPS Functional Reviews will be provided to the Center Director no later than 30 days after completion of the review. The Center will be required to submit an action plan outlining the non-compliant area along with the corrective action for compliance. OPS will review the findings within 30 days and inform the Center of the approval or disapproval of the corrective actions.

c. The Information Security Oversight Office (ISOO) maintains continuous relationships with agency counterparts on all matters relating to the Classified National Security Program and 32 CFR pt. 2004. ISOO also conducts on-site assessments to monitor agency compliance with E.O. 13526 and 32 CFR pt. 2001. Each year ISOO gathers relevant statistical data regarding each agency's security classification program. ISOO analyzes and reports this data, along with other relevant information in its Annual Report to the President. NASA follows ISOO guidance and is subject to ISOO inspections and reviews.

d. Internal and external auditors responsible for ensuring that Agency compliance and effective implementation of the E.O. 13526 will evaluate the NASA CNSI program.

P.6 Cancellation

NPR 1600.2, NASA Classified National Security Information (CNSI), dated October 11, 2011.

Chapter 1. Introduction

1.1 Overview

1.1.1 NASA generates, receives, disseminates, and maintains an enormous amount of information, much of which is of an unclassified nature with few restrictions on its use and dissemination.

1.1.2 NASA also generates, receives, stores, disseminates, and maintains CNSI under a variety of Agency programs, projects, partnerships, collaboration with other Federal agencies, academia, and private enterprises.

1.1.3 NASA establishes agency-wide procedures for the proper implementation and management of a uniform system for classifying, accounting, safeguarding, and declassifying national security information generated by, for, or in the possession of NASA.

1.1.4 Nothing in this chapter or E.O. 13526 limits the protection afforded any information by other provisions of law, including the exemptions to the 5 U.S.C. § 552, 50 U.S.C. § 3001, or 5 U.S.C. § 552a.

1.1.5 Furthermore, this chapter defines the security review requirements for programs and projects, pursuant to NPR 7120.5 and 7120.8. It establishes procedures for the creation of security classification guides (SCG), as well as requirements for reviewing permanent historical documents, pursuant to E.O. 13526, 32 CFR pt. 2001, and NPR 1441.1, before retirement into the Federal Records Centers or the National Archives and Records Administration (NARA).

1.2 Responsibilities

1.2.1 Pursuant to E.O. 13526 and 32 CFR pt. 2001, the Administrator shall demonstrate personal commitment, commit senior management, and commit necessary resources to the successful implementation of the program established under this NPR.

1.2.2 The Administrator shall designate a senior agency official (SAO) to direct and administer the information security program for managing and safeguarding CNSI in accordance with the E.O.

1.2.3 The Assistant Administrator for Protective Services has been designated as the SAO responsible for providing direction, oversight, and implementation for an Agency-wide information security program, 14 CFR pt. 1203, E.O. 13526, and 32 CFR pt. 2001 for the protection of CNSI in NASA's custody. The AA for OPS shall:

- a. Direct and administer the NASA program under which information is classified, safeguarded, and declassified.
- b. Establish Agency-wide procedures pertaining to the management of CNSI and material generated by or in the custody of NASA.
- c. Establish Agency procedures for formal classification challenges by developing a system for processing, tracking and recording formal classification challenges made by authorized holders.
- d. Periodically review procedures and systems of Headquarters, Centers, (including Component

Facilities), technical support centers, and service support centers to ensure CNSI is properly protected against unauthorized disclosure or access.

- e. Be responsible for the funding, maintenance, and operation of Information Technology systems supporting CNSI.
- f. Provide direction, oversight, and implementation of the NASA North Atlantic Treaty Organization (NATO) program in accordance with USSAN Instruction 1-07.
- g. Provide direction, oversight, and implementation of 50 U.S.C. § 2672 et seq, by developing a plan to prevent the inadvertent release of records containing Restricted Data (RD) or Formerly Restricted Data (FRD) during the automatic declassification review of records under section 3.3 of E.O. 13526.
- h. Provide direction, oversight, and implementation of E.O. 12829 and 32 CFR pt. 2004 by ensuring all the responsibilities of the Cognizant Security Agency (CSA) are met.

1.2.4 Center Directors shall, through the respective Center Chief of Protective Services (CCPS)/Center Chief of Security (CCS):

- a. Ensure proper planning and resources for the implementation of E.O. 13526 and 32 CFR pt. 2001, and managing classified information and material under the jurisdiction and custody of their respective Centers. This responsibility includes component activities at facilities or locations geographically separated from the parent Center.
- b. Ensure appropriate sanctions for security violations are coordinated with respective Center Office of Human Capital and Management, documented in Center policies, and notify OPS.
- c. Ensure the implementation of the CSA requirements at the Center level is incorporated in the acquisition and maintenance of classified contracts process.

1.2.5 The CCPS/CCS shall:

- a. Ensure an information security program for CNSI is developed, implemented, and maintained at a level sufficient to meet the requirements of this NPR and national-level requirements.
- b. Develop and implement appropriate processes and procedures for ensuring that classified NASA information meets the requirements E.O. 13526 and 32 CFR pt. 2001, and this NPR.
- c. Develop and implement appropriate processes and procedures for automatic, systematic, and mandatory review of declassification pursuant to E.O. 13526 and 32 CFR pt. 2001 subpt. D.
- d. Develop and implement procedures for the appropriate safeguarding of CNSI.
- e. Develop and implement a Center internal annual self-inspection program.
- f. Maintain the accountability of the costs associated with implementing this NPR, the E.O. 13526 and 32 CFR pt. 2001.
- g. Investigate and report sanctions, security violations, security infractions, loss, possible compromise, or unauthorized disclosure of CNSI pursuant to this NPR. Immediately notify the servicing NASA Counterintelligence office and the OPS Security Management Division Director of all actual or suspected compromises of CNSI.
- h. Raise the security threat level or develop temporary procedures to handle national security

incidents when necessary.

i. Develop and administer a security education and training program that encompasses initial training, specialized training as required (e.g., derivative classification, courier, and safe custodian training), and termination briefings for all NASA civil service employees and for contractor personnel as required in accordance with an official NASA contract.

j. Ensure the requirements of the National Industrial Security Program (NISP) are incorporated in the acquisition and maintenance of classified contracts.

1.2.6 NASA supervisors shall:

a. Ensure that performance plans for personnel whose duties significantly involve the creation or handling of classified information, including personnel who apply derivative classification markings, are appropriately designated and rated on at least one performance element related to the execution of work required for managing classified information as required by Section 5.4(7) of E.O. 13526.

b. Ensure that personnel entrusted with or handling classified information attend the required briefings, security education, and training provided by the Center Protective Services Office, the Office of Protective Services, or other Government agencies that provide classified information to NASA personnel.

1.2.7 The Center Communications Security (COMSEC) Officer shall serve as the focal point for all COMSEC issues. The Center COMSEC Account Manager (CAM) and Alternate CAM serve as the focal point for all Center COMSEC issues, in accordance with the requirements of NPR 1600.6.

1.2.8 All cleared NASA employees and contractor personnel shall:

a. Protect classified national security information from unauthorized disclosure, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person.

b. Meet safeguarding requirements prescribed by this NPR.

c. Ensure that classified information is not communicated over unsecured voice or data circuits, in public conversations, public places, or in any other manner that permits interception by unauthorized persons.

d. Maintain an annual count of all derivative classification decisions made.

e. Immediately report the following to the CCPS/CCS:

(1) Loss, possible compromise, or unauthorized disclosure of classified information or material.

(2) Known or suspected practice or condition that compromises the proper safeguarding and handling of classified information or material.

(3) Attempts by non-cleared personnel or personnel without a need-to-know to gain access to CNSI.

(4) Security violations or infractions.

f. Initial classification, downgrading, or declassification actions associated with NASA-generated information or material. Immediately report the following to their servicing NASA

Counterintelligence office:

- (1) Unusual or suspicious overtures by foreign nationals or representatives of a foreign entity to acquire CNSI or other sensitive information outside established official channels.
 - (2) Contact between cleared employees and known or suspected intelligence officers from any foreign country.
 - (3) Any contact that suggests a cleared employee may be the target of an attempted exploitation by a foreign intelligence entity.
 - (4) Any information regarding suspected or actual threats related to espionage.
- g. Challenge classification, when necessary, as a means for promoting proper and thoughtful classification actions.
- h. Forward information believed to be improperly classified to the Original Classification Authority (OCA), the Office of Protective Services, or the Center Protective Services Office for further guidance.
- i. Ensure all required training outlined in E.O. 13526, 32 CFR pt. 2001, and this NPR established for governing, accessing, protecting, accounting for, and safeguarding classified information and material is completed.

Chapter 2. CNSI Management

2.1 General

2.1.1 All personnel accessing classified information are required to have a “need-to-know” to access that level of information.

2.1.2 All personnel accessing classified information are required to have a favorable personnel security investigation, equivalent to or above the level of access required, completed in accordance with NPR 1600.3.

2.1.3 All personnel accessing classified information shall complete training, annually, in the proper procedures for handling, storing, and safeguarding classified information in accordance with the requirements of this policy.

2.1.4 Classified information is always the property of the U.S. Government and may never be perceived or construed as personal property.

2.1.5 Facility security control requirements for all CNSI areas are identified in NPR 1620.3.

2.2 Original Classification

2.2.1 Information is classified pursuant to E.O. 13526 and 32 CFR § 2001.21 by an OCA.

2.2.2 Information may be originally classified under the terms of E.O. 13526 only if all of the following conditions are met:

- a. An OCA is classifying the information.
- b. The information is owned by, produced by or for, or is under the control of NASA;
- c. The information falls within one or more of the categories of information listed in section 1.4 of E.O. 13526;
- d. The OCA determines that an unauthorized disclosure of the information would reasonably be expected to result in damage to the national security, which includes defense against transnational terrorism, and the OCA is able to identify or describe the damage.

2.2.3 If there is significant doubt about the need to classify information, do not classify it and consult OPS for guidance. This provision does not:

- a. Amplify or modify the substantive criteria or procedures for classification; or
- b. Create any substantive or procedural rights subject to judicial review.

2.2.4 Classified information is not automatically declassified because of unauthorized disclosure of identical or similar information. Do not use information that has been improperly disclosed to make classification determinations.

2.2.5 OCAs shall ensure the proper protection of foreign government information (FGI). The

unauthorized disclosure of FGI is presumed to cause damage to the national security. FGI will be protected at the U.S. Government level equivalent.

2.3 Classification Levels

2.3.1 In accordance with Section 1.2 of E.O. 13526, information may be classified at one of the three levels described in Figure 1.

Sec. 1.2. Classification Levels.

(a) Information may be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Figure 1. Classification Levels

2.4 NASA Original Classification Authority

2.4.1 Pursuant to the provisions of section 1.3 of E.O. 13526, the President has designated the Administrator as an original classification authority (OCA). Only the Administrator can delegate OCA authority to other NASA personnel. Per delegation of the Administrator in this NPR, the following NASA personnel possess OCA designation up to and including Top Secret:

- a. Deputy Administrator,
- b. Associate Administrator,
- c. Assistant Administrator for Protective Services, and
- d. Deputy Assistant Administrator for Protective Services.

2.4.2 When designated in writing by the NASA Administrator, personnel with sufficient justification may possess OCA designation up to and including Top Secret (non-delegable).

2.4.3 OCAs shall receive training in proper classification and declassification prior to originally classifying information and at least once each calendar year thereafter. Security education requirements are in Chapter 3 of this NPR.

2.5 Classification Categories

2.5.1 In accordance with Section 1.4 of E.O. 13526, specific information will only be considered for classification when its unauthorized disclosure is reasonably expected to cause identifiable or describable damage to the national security, as described in Figure 2.

Sec. 1.4. Classification Categories. Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of this order, and it pertains to one or more of the following:

- (a) military plans, weapons systems, or operations;
- (b) foreign government information;
- (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;
- (d) foreign relations or foreign activities of the United States, including confidential sources;
- (e) scientific, technological, or economic matters relating to the national security;
- (f) United States Government programs for safeguarding nuclear materials or facilities;
- (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
- (h) the development, production, or use of weapons of mass destruction.

Figure 2. Classification Categories

2.6 Application of Original Classification Authority

2.6.1 At the time of original classification of both hard copy and electronic records, OCAs will indicate the following in a manner that is immediately apparent:

- a. Classification level. The OCA shall decide which of the three classification levels defined in E.O. 13526 Section 1.2 most appropriately applies to the information.
- b. “Classified By” line. The name and position of the OCA shall be written on the “Classified By” line.
- c. Reason for the classification. The OCA shall identify the reason(s) for the decision to classify on the “Reason” line with the number 1.4 plus the letter(s) that corresponds to that classification category in section 1.4 of the E.O. 13526 (e.g. 1.4(a)).
- d. Declassification instructions. The duration of the original classification decision will be placed on the “Declassify On” line, which indicates one of the following: the date (YYYYMMDD) or event for declassification as prescribed in section 1.5 (a) of the E.O., the date that is 10 years from the date of original classification as prescribed in 1.5 (b) of the E.O., or the date that is up to 25 years from the date of original classification as prescribed in section 1.5 (b) of the E.O.

e. Establishing duration. If the classified information should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, an original classification authority will follow the sequence listed in 32 CFR pt. 2001.12 (a)(1) (i)-(iii).

(1) In accordance with the E.O. 13526, no information may remain classified indefinitely. At the time of original classification, the OCA shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information will be automatically declassified.

(2) If the OCA cannot determine a specific date or event for declassification, the information will be marked for declassification 10 years from the date of the original decision, unless the OCA otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision.

(3) An OCA may extend the duration of classification up to 25 years from the date of original of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under the E.O. 13526 are followed.

f. Date of origin of the document. The date of origin of the document will be indicated in a manner that is immediately apparent within the record.

g. A sample classification authority block for an original classification:

Classified By: <insert name and title or position of the OCA>

Reason: <insert the reason for the classification (e.g., 1.4 followed by the letter that corresponds to that classification category)>

Declassify On: <insert declassify instructions>

2.6.2 The OCA shall issue classification guidance. The OCA classification guidance may be issued in the form of an action memorandum, source document, or security classification guide (SCG). Security classification guides are the primary format for classification guidance when possible. However, other forms are acceptable when a SCG is deemed excessive or unnecessary.

2.6.3 Whenever practicable, use a classified addendum when classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

2.6.4 Overall markings along with page, component, portion markings, and use of cover sheets will conform to guidelines in accordance with E.O. 13526, 32 CFR pt. 2001, and the ISOO Booklet "Marking Classified National Security Information". If you are required to mark documents on a classified information system, classified equipment or some other unique classified item, please contact your Center Protective Services Office for specific instructions on how to mark and label each item. CNSI in the electronic environment is subject to all marking requirements.

2.6.5 Exceptional classification cases. Personnel shall not designate information as classified Confidential, Secret, or Top Secret without specific guidance from an OCA or official classification guidance. When an employee, Government contractor, licensee, certificate holder, or grantee of NASA not designated as an original classification authority obtains information believed to require original classification, the information will be protected in a manner consistent with the E.O. 13526, 32 CFR pt. 2001 and this NPR. The individual will contact the Office of Protective Services by way

of their CCPS/CCS for determination by a subject matter expert and classification authority with respect to this information.

2.6.6 In some cases, an aggregation of pre-existing unclassified items of information may require that a classification action be initiated. This act is called compilation or mosaic. Contact the Office of Protective Services by way of your CCPS/CCS to determine if a classification action is warranted.

2.7 Derivative Classification

2.7.1 The CCPS/CCS shall develop procedures for the identification, appointment, and authorization of personnel at their Center which will perform derivative classification actions.

2.7.2 Persons authorized to perform derivative classification shall be identified in writing by the CCPS/CCS, and will receive required initial and annual refresher training courses.

2.7.3 CCPS/CCS shall report all appointments of derivative classifiers to the Office of Protective Services, Security Management Division (SMD).

2.7.4 All persons with access to classified systems will be designated as derivative classifiers. Prior to gaining access to classified systems and performing derivative classification activities, authorized individuals shall:

- a. Initiate the Derivative Classifier role and the request for access to classified systems in the NASA Access Management System (NAMS); and
- b. Receive training in the proper application of the derivative classification principles.

2.7.5 Derivative classifiers will receive initial training upon designation of authority and annual refresher training thereafter. Security education requirements for the training are in Chapter 4 of this NPR.

2.7.6 Derivative classifiers who fail to take the annual clearance holder training annually will have their authority and access to classified systems suspended by the SAO until the training is completed. A waiver may be granted by the SAO if an individual is unable to receive the training due to unavoidable circumstances. Whenever a waiver is granted, the individual will receive training as soon as practicable.

2.8 Application of Derivative Classification Authority

2.8.1 At the time of derivative classification, the following will be indicated in a manner that is immediately apparent. These marking instructions apply to both hard copies and electronic records. Information derivatively classified will:

- a. Be derived from a source document(s) or SCG.
- b. Bear standard markings under the uniform security classification system and as prescribed in this NPR.
- c. Carry forward the markings, the classification authority, and declassification instructions from the source document(s) or the SCG.

2.8.2 Derivative classifiers shall not designate information as Confidential, Secret, or Top Secret without specific guidance from an OCA in the form of a source document or SCG.

2.8.3 Derivative Classifiers shall apply the following to all derivatively classified documents:

- a. Identify the person performing the derivative classification action by position and title or badge number.
- b. Identify the source documents or SCG, including the agency or office of origin and the date of the source document. In the case of multiple sources, all sources will be listed on the document or in an attachment.
- c. A sample classification authority block for derivative classifiers should appear as:

Classified By: <insert name and title or position of the derivative classifier>

Derived From : < source document, office of origin, date> or <multiple sources>

Declassify On: <insert declassify instructions>

2.8.4 Overall markings along with page, component, portion markings, and use of cover sheets will conform to guidelines in accordance with E.O. 13526, 32 CFR pt. 2001, and the ISOO Booklet “Marking Classified National Security Information”. If you are required to mark documents on a classified information system, classified equipment or some other unique classified item, please contact your Center Protective Service Office for specific instructions on how to mark and label each item. CNSI in the electronic environment is subject to all marking requirements.

2.8.5 Guidance on what is considered a derivative classification action in the electronic media realm is included in the appendix of this NPR.

2.8.6 Derivative classifiers shall track and report the number of derivative classification actions annually to ISOO in conjunction with SF 311 reporting.

2.9 Identification, Designation and Markings

2.9.1 Marking. Marking is the principal way of letting holders of information know the specific protection requirements for that information. Markings and designations serve the following purposes:

- a. Alert holders to the presence of classified information and information with restrictions on its dissemination.
- b. Identify, as specifically as possible, the exact information needing protection.
- c. Provide guidance on information sharing.
- d. Provide guidance on downgrading (if any) and declassification.
- e. Give information on the source(s) and reason(s) for classification and other restrictions.
- f. Warn holders of special access, control, or safeguarding requirements.

2.9.2 Portion Marking. A portion is ordinarily defined as a paragraph, but also includes: subjects, titles, graphics, tables, charts, illustrations, pictures, bullet statements, sub-paragraphs, classified

signature blocks, and other portions within slide presentations will be marked with the appropriate classification marking.

2.9.3 Classification designations for portion markings are:

- a. (U) for Unclassified.
- b. (C) for Confidential.
- c. (S) for Secret.
- d. (TS) for Top Secret.

2.9.4 These abbreviations are placed in parentheses before the portion to which they apply. Whenever possible, use an unclassified title or subject line.

2.9.5 Markings other than “Top Secret”, “Secret”, and “Confidential”, such as “For Official Use Only”, “Sensitive But Unclassified”, “Controlled Unclassified Information”, “Limited Official Use”, or “Sensitive Security Information”, are not to be used to identify CNSI.

2.9.6 Special Access Program (SAP) Markings. NASA employs SAP markings that are authorized and prescribed by the NASA SAP Security Guide concerning national security information for limiting access to cleared personnel having a need-to-know in the performance of their official duties.

2.9.7 Sensitive Compartmented Information (SCI). The NASA Special Security Office shall review for appropriate classification and marking any document for interagency use (MOU/MOA, memorandum, or general correspondence) involving SCI or suspected SCI produced without the benefit of a specific classification guide.

2.9.8 Foreign Government Information (FGI). Mark documents containing FGI with: “This document contains (country of origin) Information.” Mark the portions that contain the FGI to indicate the country of origin and the classification level (e.g., (Country of Origin S)). Use the Office of the Director of National Intelligence Controlled Access Program Coordination Office (CAPCO) register to locate the official abbreviation for a particular country. Substitute the country name with the words “Foreign Government Information” or “FGI” in situations where the identity of the specific government requires concealing. If the fact that information is FGI needs to be concealed, please contact the Office of Protective Services for specific instructions on how to apply appropriate markings.

2.9.9 Banner Markings. Banner markings represent the overall classification of the document. The banner markings should appear on the top and bottom of each page. Identifying the proper classification for each portion is the primary way to determine the overall classification level of a document. The banner line will specify the highest level of classification (Confidential, Secret, or Top Secret) of information contained within the document and the most restrictive control and handling markings contained within the document.

- a. The highest level of classification is determined by the highest level of any one portion within the document.
- b. The classification level in the banner line is printed in English and spelled out completely. Only the highest classification level is used on the banner line.

- c. Any other control markings (e.g., disseminating control markings) included may be spelled out or abbreviated.
- d. Banner markings always use uppercase letters.
- e. If a document contains more than one page, the banner marking will be placed at the top and bottom of the front cover (if any), the title page (if any), the first page and on the outside of the back cover (if any). Each interior page of a classified document is marked with a banner line at the top and bottom of the page. Interior pages may be marked with the highest classification level of the information contained on that page, whereas the first page of a classified document's banner reflects the highest classification level of information within the whole document.

2.10 Working Papers

2.10.1 Working papers are documents and material accumulated or created in the preparation of finished documents and material. Classifying as "working papers" is not intended as a way around the original classification procedure or temporary classification. The derivative classifier shall notify the CCPS/CCS of all working paper documents. The CCS/CCPS will ensure that the proper markings and safeguarding are being utilized to protect the information. Required markings for working papers containing classified information are:

- a. Creation date.
- b. "Working Paper" Annotation at the top and bottom.
- c. The highest level of classification contained within.

2.10.2 Working papers are required to be handled in the following manner:

- a. Protected in a manner consistent with the highest level of classification contained within the document.
- b. Controlled and marked in the manner prescribed for a finished document of the same classification when:
 - (1) Retained more than 180 days from the date of origin,
 - (2) Released by the originator outside NASA, or
 - (3) Filed permanently.
- c. Destroyed when no longer needed.

2.11 Classification Prohibitions and Limitations

2.11.1 The OCA, Declassification Authority (DCA), or derivative classifiers shall not classify information, continue to maintain a classification, or fail to declassify information in accordance with Section 1.7 of E.O. 13526.

2.11.2 Classification is prohibited when attempting to classify basic scientific research information not clearly related to the national security.

2.11.3 Classification is prohibited when attempting to reclassify information after declassification and release to the public under proper authority unless it is compliant with Section 1.7 (c) - (e) E.O. 13526.

2.12 Classification Challenges

2.12.1 In order to challenge the classification status of information, authorized holders of the classified information shall present such challenges to the OPS Security Management Division Director to the SAO. Once the challenge is received, the SMD will establish an ad-hoc committee to review the challenge and make the final Agency determination.

2.12.2 A formal challenge under this provision will be submitted in writing, but need not be any more specific than to question why information is or is not classified or is classified at a certain level.

2.12.3 Anyone with access to the information in question may challenge the classification without reprisal. Herein after the individual(s) that challenge the classification of information will be referenced as the challenger.

2.12.4 The SAO shall provide an initial written response to a challenge within 60 days. The initial written responses will acknowledge the challenge in writing and provide a date, not to exceed 120 days, by which the decision will be made. The acknowledgement will include the statement that if NASA is unable to come to a decision within the 120 days, the challenger has the right to forward the request to the Interagency Security Classification Appeals Panel (ISCAP).

2.12.5 The ad-hoc committee shall review, deliberate and decide on the classification challenge request within 120 days of receipt of the challenge.

2.12.6 Challengers and the NASA Information Security Program Committee will attempt to keep all challenges, appeals, and responses unclassified.

2.12.7 For external appeals, if no agency response is received by the challenger within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP) for a decision. The challenger may also forward the challenge to the ISCAP if NASA has not responded to an internal appeal within 90 days of the Agency's receipt of the appeal.

2.12.8 If the challenge is denied, a rationale for denial and appeal rights will be provided to the individual that submitted the challenge.

2.12.9 If the challenger does not agree with the NASA decision, he/she may refer the challenge to the ISOO for a secondary review and final determination.

2.12.10 Individuals are not subject to retribution for bringing such actions to the attention of the appropriate official or office. The classification challenge provision is not intended to prevent an authorized holder from informally questioning the classification status or particular information. Such informal inquiries should be encouraged as a means of minimizing the number of formal challenges.

2.12.11 Whenever an agency receives a classification challenge for information that has been the subject of a challenge within the past two years or that is the subject of a pending litigation, NASA is not required to process the challenge. NASA is only required to inform the challenger of this fact

and of the challenger's appeal rights.

2.12.12 Classified information that is the subject of a classification challenge will remain classified until a final decision is made to declassify it. Unclassified information will remain unclassified until a final decision made to classify it.

2.13 Declassification Authority

2.13.1 Only OCAs and persons designated as Declassification Authorities (DCA) are allowed to declassify CNSI.

2.13.2 OCAs have the authority to downgrade or declassify NASA-originated CNSI. Additionally, the originator's successor may also declassify if the successor has OCA.

2.13.3 Declassification Authorities shall meet the following criteria:

- a. The employee is nominated in writing by the Center Director/CCPS/CCS to perform functions of a NASA Declassification Authority (DCA).
- b. The DCA role is initiated in NAMS.
- c. All nominated NASA DCAs attend and successfully complete the NASA/OPS approved Declassification Authority Training Program class and the Department of Energy (DOE) training on the recognition of Restricted Data and Formerly Restricted Data (RD/FRD). Each DCA will receive a Certificate of Training approved by the OPS Assistant Administrator for Protective Services. Certified DCAs are also required to attend refresher training every three years thereafter.
- d. Additionally, each Center will have at least one DCA certified as a DOE Historical Records Restricted Data Reviewer (HRRDR). This requires attendance and successful completion of the DOE HRRDR 4-day course pursuant to the 42 U.S.C. § 2011 et seq, 50 U.S.C. §2671 et seq, and the Special Historical Records Review Plan (Supplement).

2.13.4 Classified information that has been declassified without proper authority remains classified and administrative actions will be taken to restore markings and controls, as appropriate. All such actions will be reported to the senior agency official who will promptly provide a written report to the Director of ISOO.

2.14 Declassification

2.14.1 The OPS Security Management Division Director has developed the NASA Declassification Management Plan that provides the framework for NASA compliance with E.O. 13526.

2.14.2 Automatic Declassification.

2.14.2.1 All classified records determined to have permanent historical value under title 44, United States Code, will be automatically declassified on December 31 of the year they become 25 years old regardless of whether it has or has not been reviewed, with the exception of the following:

- a. Information determined to fall within one or more of the nine exemption categories outlined in Section 3.3(b) of E.O. 13526.
- b. Information in the NASA Historical Records Declassification Guide; or

c. Information contained within a treaty or international agreement as determined by the Department of State and official of a foreign government requires protection beyond 25 years.

d. Information concerning nuclear weapons and foreign nuclear programs. Restricted Data and Formerly Restricted Data are excluded from automatic declassification. Additionally, the Secretary of Energy determines when information concerning foreign nuclear programs may be declassified.

2.14.2.2 NASA may exempt a group or file series "Exempt File Series" of records from automatic declassification CNSI, if a substantial portion of the records within the file series would be expected to remain exempt based on the provisions of E.O. 13526, Section 3.3(b) and (c). ("File series" is also described in ISOO guidance as an "integral file block.") The NASA SAO shall notify the Interagency Security Classification Appeals Panel and the Director of the ISOO, serving as Executive Secretary of the Panel, of any specific information beyond that included in a notification to the President under paragraph (c) E.O. 13526, Section 3.3 that the Agency proposes to exempt from automatic declassification. File series exemption criteria include the following:

a. A description of the information, either by reference to information in specific records or in the form of a declassification guide.

b. An explanation of why the information is exempt from automatic declassification and should remain classified for a longer period of time.

c. Except for the identity of a confidential human source or a human intelligence source and information regarding weapons of mass destruction, as provided in E.O. 13526 and 32 CFR pt. 2001, a specific date or event for declassification of the information is determined, not to exceed 50 years from the date of origin. The panel may direct the Agency not to exempt the information or to declassify it at an earlier date than recommended. The Agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

2.14.3 Information approaching 24 years and potentially meeting the requirements of 2.14.2.1 and 2.14.2.2 for automatic declassification will be submitted to OPS, SMD for review and submission to ISOO.

2.14.4 Systematic Declassification Review. The Office of Protective Services, Security Management Division shall conduct a periodic review of NASA classified programs to determine if information of permanent historical value should be declassified. This periodic review will be conducted in conjunction with the NASA fundamental classification guide review.

2.14.5 Mandatory Declassification Review (MDR).

2.14.5.1 All MDR requests are received by NASA Headquarters, Central Registry and processed through the OPS Classification/Declassification Office.

2.14.5.2 A valid mandatory declassification review request will be of sufficient specificity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. Requests for broad types of information, entire file series of records, or similar non-specific requests will be denied for processing under 32 CFR 2001 Section 2001.33.

2.14.5.3 An initial response is sent to the requestor within 60 days of receipt of the request acknowledging or denying the request.

2.14.5.4 All MDRs are processed and a final determination made within one year from the date of receipt. The MDR process includes:

- a. Conducting a line by line review of the records.
- b. Redacting information that is not releasable to the public or remains classified. The specific reason for redaction will be included for each redaction.
- c. Releasing information to the requestor, if possible. The release of information will be coordinated with reviews by other appropriate offices for sensitive but unclassified information such as export controlled data and information, personally identifiable information, etc.
- d. Coordinating referrals to other government agencies and tracking the review and referral process in the NASA Declassification Database.

2.14.6 Denials are provided to the requestor in writing, and include the reason for denial and the requestor's appeal rights. The requestor's appeal rights are as follows:

- a. Upon denial, in whole or in part, of an initial request, the requestor has the right to file an administrative appeal within 60 days of receipt of the denial.
- b. If NASA fails to respond to the request within one calendar year, then the requestor has the right to appeal to the Interagency Security Classification Appeals Panel.

2.14.7 The CCPS/CCS shall ensure Centers conduct and document annual reviews of classified holdings for automatic declassification in compliance with E.O. 13526 and 32 CFR pt. 2001.

2.14.8 When conducting annual reviews of classified holdings for automatic declassification the CCPS/CCS shall ensure DCAs are assigned to a qualified NASA Federal employee subject-matter expert that will assist them in declassification efforts.

2.15 Access to CNSI

2.15.1 At a minimum, NASA personnel and other individuals associated by contract or other agreement shall meet the following criteria for accessing CNSI in accordance with E.O. 12968 and E.O. 13526:

- a. Possess a personnel security clearance commensurate with the required access.
- b. Have a justified need-to-know.
- c. Sign an official nondisclosure statement (SF 312) witnessed by a NASA security official, an approved facility security officer, or other approved official.

2.15.2 Access to Restricted Data and Formerly Restricted Data. NASA cleared personnel requiring access to DOE RD/FRD shall submit a request through NAMS. Specific justification for access is required for approval. When the NAMS process is initiated and the justification is accepted, the NASA RD Management Official will prompt the requestor to complete DOE form 5631.18. The RD Management Official will forward the signed form and the justification to the NASA Central Adjudication Facility for submission to DOE. All personnel granted DOE Q or L clearances will receive training.

2.16 Limited Access to CNSI by Non-U.S. Citizens

2.16.1 The AA, OPS, or designee, may authorize the granting of a Limited Access Authorization (LAA) to a non-U.S. citizen (including lawful permanent residents (LPR)) for specific information up to the Secret level if:

2.16.1.1 It has been determined that the non-U.S. citizen possesses unique or unusual skills or expertise that is urgently needed to support a specific NASA mission; or,

2.16.1.2 It has been determined that no cleared or clearable U.S. citizen can support the NASA mission.

2.16.2 Process for Requesting an LAA. NASA organizations shall submit a written request for an LAA to the CCS/CCPS. The request will include:

- a. The individual's name, date and place of birth, position title, and current citizenship.
- b. A statement explaining the compelling reasons for the request and why it is impractical or unreasonable to use U.S. citizens to perform the required work or function, including any time constraints.
- c. A statement of the individual's special expertise.
- d. A statement explaining how access will be limited to a specific program or project, and how access will be limited and physical custody of CNSI precluded.
- e. A statement that the CNSI to be accessed is releasable to the individual's country of citizenship or that an export license has been obtained.

2.16.3 The CCS/CCPS shall evaluate the request with the Center International Visitor Coordinator (IVC) and Center Export Administrator (CEA) to identify any potential issues and make an endorsement recommendation and forward to the AA, OPS for LAA review.

2.16.3.1 The AA, OPS shall coordinate with OIIR and other relevant offices or Agencies to determine concurrence or non-concurrence prior to granting the LAA.

2.16.3.2 The AA, OPS shall provide a final response to the CCS/CCPS and the requesting organization.

2.16.4 If an LAA is initiated by a NASA cleared contractor performing on a NASA classified contract, only the DSS/DoD CAF or successor organization has the authority to grant the LAA. The following procedures shall apply.

2.16.4.1 The cleared contractor's Facility Security Officer shall submit a written request for an LAA to the CCS/CCPS that includes all information from section 3.10.2.1.

2.16.4.2 The CCS/CCPS shall ensure the contract is current and has a current DD-254 in place.

2.16.4.3 The requirements in sections 3.10.2.2 through 3.10.2.5 shall be followed.

2.16.4.4 If acceptable, the AA, OPS shall endorse and submit the request to DSS to grant the LAA.

2.16.4.5 The AA, OPS will receive the DSS endorsement and forward the final response to the CCS/CCPS and the contractor.

2.16.5 Center OPS shall ensure:

- a. An investigation sufficient for access to Secret and a favorable adjudication is obtained before access is granted. The granting of interim or temporary access pending completion of the investigation is prohibited.
- b. Denied requests are returned to the requestor with an explanation of the denial.
- c. A copy of the concurrence or non-concurrence will be retained by OPS.
- d. The non-U.S. citizen nominated for the LAA signs a nondisclosure agreement if the LAA is granted.

2.16.6 Requests for access to CNSI owned by another agency shall be coordinated with and approved by that agency.

2.17 Accountability and Control of CNSI

2.17.1 All classified information is strictly accounted for and, for Top Secret only, covered by a continuous chain of signature receipts and inventory records. This chapter details the minimum requirements for accountability and control. Centers are encouraged to implement additional controls when appropriate.

2.17.2 Each Center will have an information management system and set of written procedures to control the classified information in its possession. The system or procedures will contain specific requirements to account for and safeguard CNSI. The system will be sufficient to reasonably preclude the possibility of the loss or compromise of CNSI.

2.17.3 A trained Top Secret Control Officer (TSCO) and alternate shall be designated, in writing, by the CCPS/CCS. The TSCO will ensure that all Center Top Secret material is accounted for, protected, and transmitted under a chain of receipts using NF 387, or other Office of Protective Services approved documentation, identifying each individual with custody of the material.

2.17.4 Each item of Top Secret material, will be numbered in series. The copy number is placed on Top Secret documents and on all associated transaction documents. This is applicable to all media types, i.e. electronic and paper.

2.17.5 A record of Top Secret material produced is maintained when the material is: a. Completed as a finished document,

- b. Retained for more than 180 days after creation, regardless of the stage of development, or
- c. Transmitted outside the facility.

2.17.6 A trained Classified Material Control Officer (CMCO) and alternate shall be designated in writing by the CCPS/CCS. The CMCO will ensure that all Center CNSI material is received by an authorized person and safeguarded in accordance with E.O. 13526, and this NPR.

2.17.7 The CMCO is responsible to the CCPS/CCS for the Center Security Control Point (SCP) and oversight of the Document Control Points (DCP) within the Center and/or facilities.

2.17.8 Establishment of SCP. One SCP, operated by the CMCO, is established within each Center or

facility that has a requirement to handle classified information. The SCP will be designated in writing within the local security procedural requirements. All incoming and outgoing classified information will be processed through the SCP with the following exceptions: SCI material and classified messages that are handled, processed, and stored within secure telecommunications spaces.

2.17.9 Document Control Point (DCP). Centers with significant volumes of classified material and where the SCP serves many organizations, each organization which has custody of classified material will establish a Document Control Station Official (DCSO) run by a Document Control Point Officer. Organizationally, this station may be established at the office, division, staff, or lower level, depending upon the circumstances. Creation of such stations will be coordinated with the CMCO and approved in writing by the CCPS/CCS.

2.18 Accountability Logs

2.18.1 NASA does not require the continuous chain accountability logs of Confidential or Secret material other than accounting for its receipt, creation, and destruction. However, the OPS Security Management Division Director recognizes that continuous chain accountability is a best practice in order to ensure and account for all classified material during a suspected or actual loss or compromise.

2.18.2 All Top Secret material will be accounted for throughout its life cycle. Records will be maintained for all Top Secret material and retained for five years after final disposition. These records will be maintained at the SCP for any accountable information, which is received, generated, reproduced, transmitted, downgraded, or destroyed. A Classified Document Control Log will be used for this purpose.

2.18.3 The Classified Document Control Log maintained at the SCP will, at a minimum, reflect the following for Top Secret:

- a. Date of receipt and date of origination.
- b. Agency/installation from which received or by which originated.
- c. Classification level of the material.
- d. A brief unclassified title or description of the material.
- e. The date of declassification or downgrading.
- f. Page count.
- g. Control number assigned. Each copy of a classified document or item will have its own control number. Copy numbers will not be used as part of the control number.
- h. Information indicating the location or local holder of the material. (Local holders/custodians shall have some form of signature receipt on file acknowledging that they have custody of the material.)
- i. Disposition and date for all material destroyed, downgraded, declassified, or dispatched outside the installation.

2.18.4 The Classified Document Control Log maintained at the SCP will, at a minimum, reflect the

following of Secret and Confidential:

- a. Classification level of the material.
- b. Control number assigned.
- c. Disposition and date for all material destroyed, downgraded, declassified, or dispatched outside the DCSO.

2.18.5 Signed receipts, destruction reports and accountability logs will be retained for five years after final disposition.

2.18.6 Top Secret disclosure records.

2.18.6.1 A disclosure record of all persons who are afforded access (including visual, oral, and record copies) to Top Secret information (except safe combinations) is maintained. This record will show the names of all individuals given access and the date of such access. To comply with this requirement, a Top Secret Cover Sheet (Form SF 703) will be attached to all Top Secret information in document form. For access given orally, a log listing the required information will be maintained. At a minimum, the Disclosure Record Sheet will provide:

- a. Information reflecting the document being disclosed.
- b. Individual to whom the information is being disclosed.
- c. Organization and telephone number.
- d. Date the information is disclosed.

2.18.6.2 Records are retained for five years from the date of final disposition.

2.19 Handling of Incoming Classified Material

2.19.1 The CCPS/CCS shall provide written procedures for the handling of incoming classified material. When a Center/facility receives incoming mail, bulk shipments, and other classified materials delivered by messenger, the following controls are implemented:

- a. All classified material is logged and delivered immediately to the SCP or properly safeguarded in accordance with this NPR until delivery to the SCP can be affected.
- b. All Registered, USPS Express Mail, and contract overnight delivery packages are delivered unopened to the SCP and protected as Secret material until determined otherwise.
- c. All personnel who open official mail of any sort shall immediately deliver any classified material to the SCP. Outer wrappers along with the unopened inner wrapper will be delivered to the SCP. If an individual opens mail, which is not correctly packaged, causing exposure to non-cleared or unauthorized individuals, the material will be delivered to the SCP, and the CCPS/CCS will be notified. The CCPS/CCS will investigate and submit a report of incidents involving classified material outlined in paragraph 2.29.2.1 of this NPR.
- d. All incoming packages containing classified material will be inspected for tampering. If tampering is discovered, it will be reported to the CCPS/CCS who will conduct necessary inquiries. The contents of the package will be checked against the enclosed receipt.

e. Incoming classified material that does not fall under the Classified Management Computer system, such as a large device or piece of equipment, will be processed in accordance with the local Center security procedures established for that type of material.

2.20 Record of Destruction

2.20.1 An accurate record of destruction of classified material is as important as the manner of its destruction. Proper accounting procedures, together with accurate records of destruction, provide evidence of the proper disposition of classified material. Records of destruction are retained for five years from the date of destruction. Approved methods for destruction are in section 2.32.6 of this NPR.

2.20.2 A record of destruction is required for all Top Secret material designated for destruction. The destruction record will indicate the date the material was actually destroyed, the control number, the short title or a description of the material destroyed consistent with the description indicated in the control log, and the printed names and signatures of the official actually performing the destruction and a witness.

a. Two-person integrity is implemented for the destruction of Top Secret material and will be accomplished by at least one Center Security Specialist and one other person authorized with the need to know to access the information. Both individuals will sign the destruction receipt. Either the control log or a separate destruction report may be used for this purpose.

2.20.3 Secret and Confidential material is destroyed only by an authorized individual approved by the Center Protective Services Office.

2.21 Inventory Requirements

2.21.1 Two appropriately cleared individuals shall conduct inventories for Top Secret material. One of the individuals should be the control officer for the material.

2.21.2 An inventory is a visual sighting of each item of accountable material. All documents held are checked to ensure that they are entered into accountability, and all documents entered into accountability will be sighted, including those items signed out on local custody. If no disposition can be determined, a security incident report involving classified material will be submitted in accordance with section 2.35 of this NPR.

2.21.3 All Top Secret materials are inventoried upon change of custodian or semiannually. Semiannual inventories may be combined with change of custodian inventories. Accountability records will also be reviewed for accuracy and continuity. Section 2.18 contains a complete listing of required page checks.

2.21.4 Secret and Confidential material will be protected and safeguarded from persons without authorized access or need to know in accordance with E.O. 13526, 32 CFR pt. 2001 and this NPR.

2.21.5 The Center shall retain a record of all Top Secret inventories for at least five years. An inventory and a report of the results, including any discrepancies discovered, will be forwarded annually to the cognizant CCPS/CCS. Although an inventory of Top Secret holdings is required on a semiannual basis, a written report to the CCPS/CCS is only required annually unless discrepancies are discovered. Although the Top Secret inventory is only reported annually, local documentation of

all inventories will be maintained at the installation as described above.

2.21.6 Upon change of custodian, all Top Secret material is transferred to the new custodian. A joint inventory will be conducted, accounting for each item. Both parties will sign the report documenting the completion of the inventory.

2.21.7 Changes and corrections. The custodian, under the direction of the CMCO, shall be responsible for the entry of all changes and corrections to the material in their custody. A Publication Change Checklist is used for all changes entered. Completed checklists will be retained until the publication is destroyed or superseded.

2.22 Top Secret Inventory

2.22.1 A page check will be conducted on all Top Secret material. Page checks involve visually sighting each page in a document, verifying its presence against a list of effective pages (if applicable), and ensuring that the page is from the original document. In the absence of a list of effective pages, the document will be examined for continuity. After each page check, the individual will sign the page check record (except for page checks prior to destruction). If one does not exist, a page check record will be produced locally and kept with the publication. The record will identify the publication, the name of the individual conducting the page check, discrepancies noted, and the date of the check.

2.22.2 Page checks on Top Secret material are conducted at least annually and on the following occasions: initial receipt, page change, classification change, change of custodian, inventory, and destruction.

2.22.3 No page checks are required for Secret or Confidential material.

2.23 Guidelines for Electronic Classified Information Processing

2.23.1 CNSI in the electronic environment is:

- a. Subject to all the requirements of the E.O. 13526, 32 CFR pt. 2001, and this NPR.
- b. Marked with proper classification markings to the extent that such marking is practical, including portion marking, overall classification, "Classified By," "Derived From," "Reason" for classification (originally classified information only), and "Declassify On."
- c. Marked with proper classification markings when appearing in an electronic output (e.g., database query) in which users of the information will need to be alerted to the classification status of the information.
- d. Marked in accordance with derivative classification procedures, maintaining traceability of classification decisions to the original classification authority. In cases where classified information in an electronic environment cannot be marked in this manner, a warning will be applied to alert users that the information may not be used as a source for derivative classification and to provide a point of contact and instructions for users to receive further guidance on the use and classification of the information.

2.23.2 Markings on Classified E-mail.

- a. E-mail transmitted on, or prepared for transmission, on classified systems or networks is configured to display the overall classification at the top and bottom of the body of each message. The overall classification marking string for the e-mail reflects the classification of the header and body of the message. This includes the subject line, the text of the email, a classified signature block, attachments included in the messages, and any other information conveyed in the body of the e-mail. A single linear text string showing the overall classification and markings is included in the first line of text and at the end of the body of the message after the signature block.
- b. Classified e-mail is portion marked to reflect the highest level of information contained in that portion. A text portion containing a uniform resource locator (URL) or reference (i.e., link) to another document will be portion marked based on the classification of the content of the URL or link text, even if the content to which it points reflects a higher classification marking.
- c. Subject lines are portion marked to reflect the sensitivity of the information in the subject line itself and not reflect any classification markings for the e-mail content or attachments. Subject lines and titles are portion marked before the subject or title.
- d. When forwarding or replying to an e-mail, individuals shall ensure that, in addition to the markings required for the content of the reply or forward e-mail itself, the markings for the overall classification and declassification instructions of the entire string of e-mails and attachments are also reflected. This will include any newly drafted material, material received from previous senders, and any attachments.

2.23.3 Each CCP/CCS is responsible for providing a count of all original (where applicable) and derivative classification actions electronically processed throughout the year in accordance with SF 311 at the end of the fiscal year. Do not count products classified by another agency and do not count any reproductions or copies. Instruction “Guidelines for SF 311 Data Collection” should be referenced for assistance.

- a. The CCPS/CCS shall establish written procedures to ensure that an accurate record of electronic processing done throughout the year is maintained by each derivative classifier to assist in the completion the SF 311 at the end of the fiscal year.

2.23.4 Marking Web Pages with Classified Content.

- a. Web pages are classified and marked on their own content regardless of the classification of the pages to which they link. Any presentation of additional web material links are also marked based on its own content.
- b. The overall classification marking string for every web page will reflect the overall classification markings (and any dissemination control or handling markings) for the information on that page.
- c. Classified web pages are portion marked and contain a classification authority block. The block may appear as a single linear text string instead of the traditional appearance of the three lines of text.

2.24 Storage of CNSI – Security Containers and Vaults

2.24.1 The General Services Administration (GSA) establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, and other associated security devices suitable for the storage and protection of CNSI against forced, covert, and

surreptitious entry.

2.24.2 All classified documents and material under the jurisdiction, possession, control, and ownership of NASA are stored in a “General Services Administration Approved” security container with a combination lock meeting Federal Specification FF-L-2740 or a facility/room with sufficient physical and procedural security measures to preclude unauthorized access.

2.24.3 Whenever new security equipment is procured, it will conform to the standards and specifications established by GSA and will, when available, be procured through the Federal Supply System.

2.24.4 Deployment, use, and maintenance of security containers, vaults, and secure areas designed for storage or daily use and discussion of CNSI is centrally managed by the CCPS/CCS to ensure their use is consistent with Agency and Center policies and procedures for storage and accountability of CNSI. The CCPS/CCS will:

a. Ensure only GSA-approved security containers, designed specifically for storage of CNSI, are used for the storage of CNSI.

b. Ensure GSA-approved security containers and vaults clearly display the following labels:

(1) GSA-approved label.

(a) Indicates that the container has been tested and certified by the GSA.

(b) On containers manufactured after October 1990, label is silver with red lettering.

(c) On containers manufactured prior to October 1990, label is either silver with black lettering or black with silver lettering.

(2) Test certification label.

(a) Identifies the class of container and the amount of time the container protects against forced, covert, and surreptitious entry.

(b) Displayed on the external side of the control door (drawer or drawer with the lock).

(3) Number label.

(a) Serves as container serial number.

(b) Displayed on front face of container.

c. Maintain a current database of all Center-wide security containers and vaults to include (at a minimum):

(1) Assigned Center-specific security container or vault.

(2) Location of container or vault.

(3) Custodian/Alternate custodian.

(4) Highest classification level of information stored.

d. Ensure repair and recertification of a GSA-approved container as required by Federal Standard 809-B if its GSA-approved label is missing or if the structural integrity of the container has been

compromised.

e. Ensure approved containers and vaults are used only for storage of CNSI and necessary unclassified reference materials. Storage of unclassified materials is kept to the absolute minimum.

f. Ensure high-value items that are targets of theft such as funds, weapons, and precious metal are not to be stored in the same container as classified materials.

g. Ensure approved security containers and vaults are properly tagged “Not for Storage of Classified Material” by the CCPS/CCS prior to use in storage of non-classified material.

h. Establish procedures to remove unneeded security containers that are removed from service and retained for future use or properly disposed of and ensure combinations are set back to “factory settings”, 50-25-50.

i. Ensure locking mechanisms are properly outfitted with or upgraded to appropriate federally mandated “X” series locks under the following circumstances:

(1) When the security container or vault is newly procured or reentered into service.

Note: For storage of classified material: containers and vaults are inspected, reconditioned as necessary, recertified, and designated in writing by the Center locksmith and acknowledged by the CCPS/CCS prior to being reentered into service.

(2) When the locking system requires replacement.

(3) When the container or vault is used to store Top Secret, COMSEC, Special Access Required, or SCI information and material.

2.24.5 Combinations.

2.24.5.1 Combinations are changed when first placed in service and then as needed whenever a person knowing the combination is transferred or terminated from employment or is no longer authorized access to the classified material stored in the equipment or area; whenever it is possible that the combination may have been subjected to compromise; or whenever the security storage equipment or security area has been found unsecured and unattended.

2.24.5.2 Combinations are recorded on SF 700, Security Container Information.

a. The SF 700 provides the names, addresses, and telephone numbers of employees who are to be contacted if the security container to which the form pertains is found open and unattended.

(1) Part 1 is affixed on the inside of the locking drawer of the security container.

b. The form also includes the means to maintain a current record of the security container’s combination and provides the envelope to be used for storage of the combination (parts 2 and 2A).

c. Combinations are classified at the highest level of the classification of the information authorized for storage in the security container.

d. SF 700 combination envelopes (parts 2 and 2A) are maintained by the CCPS/CCS. Different storage requirements may apply when the combinations are for information at the SCI/SAP levels.

e. A new SF 700 is completed each time the combination to the security container is changed.

2.25 Forms

2.25.1 Records are kept for all security containers, vaults, and secure rooms that are used to store classified material. The SF 700 and SF 702 are required for every storage container. The SF 701 is required for all work areas where CNSI is processed.

a. SF 700, Security Container Information.

(1) Section 2.23.7 of this NPR describes proper implementation of this required form.

b. SF 701, Activity Security Checklist.

(1) Provides a systematic means to make a thorough end-of-day security inspection for a particular work area where CNSI is processed to ensure that the work areas are secured at the end of each working day.

(2) Allows for employee accountability in the event that irregularities are discovered.

(3) Is intended to be used for secure areas where CNSI is processed.

c. SF 702, Security Container Check Sheet.

(1) Provides a record of the names and times that persons have opened, closed, or checked a particular container that holds classified information.

(2) Is used to log each opening and closing of a security container or vault. It is placed on the container or on the door of the secure area.

(3) Is also used for the purpose of security checks of a container or vault.

d. Cover Sheets. Cover sheets serve as a shield to protect classified information from inadvertent disclosure and to alert observers that classified information is attached to it.

(1) SF-703 is used for Top Secret information.

(2) SF-704 is used for Secret information.

(3) SF 705 is used for Confidential information.

e. Labels. Labels are used to identify and protect electronic media and other media that contains or processes classified information. These labels are used instead of cover sheets for media other than documents. Labels are also used to identify information systems, printers, copiers and facsimile machines that are approved to process classified information. Use the label that is the highest classification of the information contained on the media or approved to process.

(1) SF 706 is used for Top Secret media.

(2) SF 707 is used for Secret media.

(3) SF 708 is used for Confidential media.

(4) SF 710 is used for Unclassified media. A mixed environment in which classified and unclassified information are being processed or stored, the SF 710 is used to identify electronic media and other

media (information systems, printers, copiers, multifunction devices, and facsimile machines) that contain unclassified information.

2.26 Storage of NATO Classified Information and FGI

2.26.1 NASA has been designated as a NATO Sub registry by the U.S. Army Headquarters, Central U.S. Registry. NASA also has designated NATO User Offices at approved Centers. The NATO Control Officer and Alternate Control Officer are located in the OPS Security Management Division. If your work requires access to NATO classified information, please contact your Center Protective Services Office or the OPS Security Management Division Director.

2.26.2 Safeguard NATO classified information in compliance with USSAN Instruction 1-07. NATO and FGI should be stored separately from other classified information. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. Safeguarding standards may be modified if required or permitted by treaties or agreements or for other obligations, with prior written consent of the National Security Authority of the originating government. 32 CFR § pt. 2001.54 should be referenced for more detail on how to protect FGI.

2.27 Emergency Authority

2.27.1 Senior Agency management or any designee may prescribe special provisions for the dissemination, transmission, safeguarding, and destruction of classified information during certain emergency situations. In emergency situations in which there is an imminent threat to life or in defense of the Homeland, Agency heads or designees may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

- a. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose.
- b. Limit the number of individuals who receive it.
- c. Transmit the classified information via approved Federal Government channels by the most secure and expeditious method to include those required in 32 CFR pt. 2001, subpt. C or other necessary means when time is of the essence.
- d. Provide instructions on safeguarding information. Physical custody of classified information will remain with an authorized Federal Government entity in all but the most extraordinary circumstances.
- e. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information. Obtain a signed nondisclosure agreement.
- f. All disclosures of classified information will be reported to the CCPS/CCS and the originator immediately or at the earliest opportunity. The CCPS/CCS will notify the OPS Security Management Division Director and provide the following information as soon as possible:
 - (1) A description of the disclosed information.
 - (2) Identity of the individual who authorized the disclosure.

- (3) To whom the information was disclosed.
- (4) How the information was disclosed and transmitted.
- (5) Reason for the emergency release.
- (6) How the information is being safeguarded.
- (7) A description of the briefing provided and a copy of the signed nondisclosure agreements.

2.28 Reproduction of CNSI

2.28.1 Reproduction of classified information and material is kept to a minimum. Only equipment designated by the CCPS/CCS is authorized to reproduce classified information. Each Center CCPS/CCS shall develop and implement written procedures to ensure that the following requirements, as a minimum, are met:

- a. Reproduction is accomplished by authorized persons knowledgeable of the procedures for classified reproduction.
- b. Protect classified information during reproduction.
- c. Adequately clear equipment after reproduction.
- d. Copies of classified information are subject to the same controls as the original information and incorporated into the Center CNSI accountability system.
- e. Safeguard overruns, waste, and blank copies generated during the clearing of reproduction equipment by handling material as “classified” and destroy copies accordingly.
- f. Ensure security procedures are provided for reproducing classified information by other technical means.

2.28.2 The CCPS/CCS shall ensure that all equipment hard drives used in machines for reproduction are wiped or destroyed in accordance with standards used to erase classified information.

2.29 Hand-Carrying and Receipting of Classified Material

2.29.1 CNSI is transmitted in a manner that ensures protection of the material. A receipt will be required whenever CNSI material is transmitted using an authorized NASA official, entered into the U.S. Postal System or via authorized contract courier, transmitted off the Center by any means, transmitted to a non-NASA activity, or when the transmitting custodian wishes to verify change of custody.

2.29.2 The CCPS/CCS shall develop courier briefings as described in Chapter 4 of this NPR.

2.29.3 The OPS Security Management Division Director or the CCPS/CCS shall appoint a NASA employee or contractor to be a designated courier of CNSI when it is essential for that NASA employee or contractor to hand-carry such information within or outside HQ or a Center. The hand-carrying of CNSI on an airplane is pre-coordinated with the CCPS/CCS at least 3 weeks prior to departure.

2.29.4 Couriers may also be required for symposiums where transport, control, and access to CNSI may be necessary, for “cleared” conference or symposium attendees, including other Agency personnel or for NASA contractors holding NASA security clearances for a classified contract under a DD Form 254.

2.29.5 Authorization is provided to the designated courier on a NASA-approved Courier Authorization Card or NASA letterhead stationery, marked “Valid only in the United States of America,” and will include a specific expiration date and the names and home telephone numbers of one NASA Security Specialist who may be contacted if the designated courier is challenged to open the materials by non-NASA personnel (police, other Government officials, or airline personnel).

2.29.6 While the NASA Courier is going through or awaiting approval to clear airport security, the classified information will be kept within an appropriate container and within the custody of the courier at all times and not opened. The NASA Security Specialist will work with the airport security manager to resolve the situation or instruct the individual to return the classified material to the Center if the situation cannot be resolved in a timely manner.

2.29.7 Methods of Transportation within a Center.

2.29.7.1 The TSCO, custodian, or other employee having a Top Secret clearance and designated by either TSCO or the CCPS/CCS, shall personally hand-carry Top Secret information within a Center. SF 703 will be attached to all Top Secret information in document form or SF 706 will be attached to all Top Secret media.

2.29.7.2 Classified information is transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that timely delivery to the intended recipient is accomplished. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized to store classified information in accordance with this directive. When traveling within a building, classified material is hand-carried, covered with the appropriate coversheets or labels with the recipient and sender name written on the cover page, enclosed in a single envelope or other suitable package, and carried in a briefcase or other container. When hand carrying classified material, the individual shall proceed directly to the intended destination. Restroom breaks, coffee breaks, and any other detour, are not permitted when hand carrying classified material.

2.29.7.3 Transmitting between buildings of a Center or outside the facility, Top Secret, Secret, and Confidential information is double-wrapped, appropriately marked, addressed with the recipient and sender address on the inner envelope, and appropriate cover sheets or labels attached to the classified material.

2.29.7.4 Additional measures may be established by the CCPS/CCS to control access to any CNSI by an unauthorized person during transmission.

2.29.7.5 Such material is transmitted inside a Center by hand-delivery from a courier briefed employee possessing a clearance at least as high as the category of classification of the material involved.

2.29.8 Hand Carrying Outside a Center.

2.29.8.1 The hand carrying of CNSI outside a Center is coordinated with the SCP or DCP so the appropriate receipting and wrapping of the material can take place.

2.29.8.2 CNSI transmitted outside a Center is enclosed in two layers, both of which provide reasonable evidence of tampering and which conceal the contents. The inner cover is a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover is sealed and addressed with no identification of the classification of its contents.

2.29.8.3 A receipt is attached to or enclosed in the inner cover. The receipt will identify the sender, the addressee, and an unclassified description of the materials being transmitted. The receipt will be signed by the recipient and returned to the sender, who will retain it for five years.

2.29.8.4 A suspense system is established to track transmitted documents until a signed copy of the receipt is returned. If signed receipts are not received within 30 days of transmission of the material, the CMCO will report the non-receipt to the CCPS/CCS.

2.29.8.5 When the material is of a size, weight, or nature that precludes the use of envelopes, the materials used for packaging will be of such strength and durability to ensure the necessary protection while the material is in transit.

2.30 Transmission of Classified Material

2.30.1 The term “transmission” refers to any movement of classified material or material from one place to another. Unless a specific kind of transportation is restricted, the means of transportation is not significant.

2.30.2 Classified material is transmitted and received in an authorized manner, which ensures that evidence of tampering can be detected; inadvertent access can be precluded; and provides a method that assures timely delivery to the intended recipient. Persons transmitting classified material are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with the E.O. 13526, 32 CFR pt. 2001 and this NPR.

2.30.3 Classified material is transmitted either in the custody of an appropriately cleared individual, by an approved system or courier, or otherwise in accordance with the provisions of this NPR. The NASA Special Security Officer (SSO) is responsible for providing instructions concerning the transmission of Sensitive Compartmented Information (SCI) material. Contact your Center Special Security Officer to receive policy and guidance for SCI.

2.30.4 The carrying of classified material across international borders is not permitted unless arrangements have been made that precludes customs, postal, or other inspections. In addition, foreign carriers will not be used unless the U.S. escort has physical control of the classified material.

2.30.5 Transmittal documents and Agency-prescribed special markings will indicate on their face/cover the highest classification level of any classified information attached or enclosed. The transmittal is to also include, conspicuously, on its face/cover the following or similar instructions as appropriate:

- a. “Unclassified When Classified Enclosure Removed.”
- b. “Upon Removal of Attachments, This Document Is (Classification Level).”

2.30.6 Top Secret transmission.

2.30.6.1 Internal mail and messenger system of an installation, U. S. Postal Service, and commercial

delivery services are not authorized for the transmission of Top Secret material. Top Secret material is only transmitted by:

- a. Defense Courier Service (DCS).
- b. Department of State Courier System.
- c. Appropriately cleared NASA civilian personnel or cleared NASA contractor specifically designated as a courier.
- d. Telecommunications systems specifically approved for transmission of Top Secret material.

2.30.7 Secret transmission.

2.30.7.1 Transmission of Secret material may be affected by:

- a. Any of the means approved for the transmission of Top Secret, except that Secret material, other than that containing cryptologic information, which may be introduced into the DCS only when the control of such material cannot otherwise be maintained in U.S. custody. When the Department of State Courier System is used for transmission of Secret material, the Secret material will be sent by registered mail to the State Department Pouch Room.
- b. U.S. Postal Service (USPS) registered mail within and between the 50 states and territories of the U.S.
- c. USPS Express Mail Service, which may be used between NASA units and contractors within and between the 50 United States and its Territories. USPS Express Mail is authorized only when it is the most cost effective method or when time/mission constraints require it. The package will be properly prepared for mailing. The USPS Express Mail envelope will not serve as the outer wrapper. The package will be double wrapped as required then placed in the USPS Express Mail envelope. Under no circumstances will the sender execute the "Waiver of Signature and Indemnity" section of the USPS Express Mail Label for classified material. This action can result in drop-off of a package without the receiver's signature and possible loss of control.
- d. Federal Express (FedEx), which the CCPS/CCS may authorize for overnight delivery of material for the Executive Branch when an urgent requirement exists for overnight delivery within the 50 United States and its Territories. The sender is responsible for ensuring that an authorized person be available to receive the delivery. The package will only be addressed to the recipient by name. The release signature block on the receipt label will not be executed under any circumstances. The use of street-side collection boxes is prohibited. COMSEC, NATO, and FGI will not be transmitted in this manner.
- e. Secret material will be transmitted by USPS registered mail, Army, Navy, or Air Force Postal Service facilities and will not pass through a foreign postal system, any foreign inspection, or via foreign airlines. The material will remain under U.S. control. The Center Protective Services Information Security Specialist will ensure that classified material sent to U.S. activities overseas will be appropriately prepared and transported by an approved carrier. If the material is introduced into a foreign postal system, it has been subjected to compromise.
- f. Qualified carriers authorized to transport Secret material via a Protective Security Service under the 32 CFR pt. 2004, within U.S. boundaries only. This method is authorized only when the size, bulk, weight, nature of the shipment, or escort considerations make the use of other means impractical.

g. Other carriers under escort of appropriately cleared personnel. The Center Protective Services Information Security Specialist will determine what carrier service should be used based on the availability of service providers in the area. Carriers include Government and Government contract vehicles, aircraft, ships of the U.S. Navy, Federal employee-manned U.S. Naval Ships, and ships of U.S. registry. Appropriately cleared operators of vehicles, officers of ships, or pilots of aircraft who are U.S. citizens may be designated as escorts, provided the control and surveillance of the carrier is maintained on a 24-hour basis. The escort will protect the shipment at all times, through personal observation or authorized storage to prevent inspection, tampering, pilferage, or unauthorized access until delivery to the consignee. However, observation of the shipment is not required during the period if stored in an aircraft or shipped in connection with flight or sea transit, provided the shipment is loaded into a compartment that is not accessible to any unauthorized persons aboard or loaded in specialized shipping containers, including closed cargo containers.

h. Telecommunications systems specifically approved for the transmission of Secret material.

2.30.8 Confidential transmission.

2.30.8.1 Transmission of Confidential material may be effected by:

a. Any of the means approved for the transmission of Secret material.

b. USPS registered mail.

2.30.9 Transmission of NATO classified information. The NASA Sub registry is the only entity that can transmit (send and/or receive) NATO classified information. Please contact the OPS Security Management Division Director for further guidance.

2.30.10 Release of U.S. Classified Information to Foreign Governments.

2.30.10.1 Subsequent to a determination by the OPS Security Management Division Director that classified material may be released to a foreign government, the material is transferred between authorized representatives of each government in compliance with the provisions of this chapter. To ensure compliance, each contract, agreement, or other arrangement that involves the release of classified material to foreign entities will either contain transmission instructions or require that a separate transportation plan be approved by the OPS Security Management Division Director prior to release of the material. Classified material is transmitted only:

a. To an embassy or other official agency of the recipient government that has extraterritorial status.

b. For on-loading aboard a ship, aircraft, or other carrier designated by the recipient government at the point of departure from the U.S. or its Territories or possessions. At the time of delivery, a duly authorized representative of the recipient government will be present at the point of departure to accept delivery, ensure immediate loading, and to assume security responsibility for the classified material.

2.30.10.2 Classified material to be released directly to a foreign government representative is delivered or transmitted only to a person who has been designated in writing by the recipient government as its officer, agent, or employee. This written designation will contain assurances that such person has a security clearance at the appropriate level and that the person will assume full security responsibility for the material on behalf of the foreign government. The recipient will be required to execute a receipt for the material, regardless of the level of classification.

2.30.10.3 Each contract, agreement, or arrangement, which contemplates transfer of U.S. classified material to a foreign government within the U.S. or its Territories, will designate a point of delivery in accordance with subparagraph 2.13.1.a or 2.13.1.b. If delivery is to be made at a point described in subparagraph 2.13.1a the contract, agreement, or arrangement will provide for U.S. Government storage or storage by a cleared contractor at or near the delivery point. U.S. classified material may be temporarily stored in the event the carrier designated by the recipient foreign government is not available for loading. Any storage facility used or designated for this purpose will afford the U.S. classified material the appropriate level of protection required.

2.30.10.4 If U.S. classified material is to be delivered to a foreign government within the recipient country, it will be transmitted in accordance with this chapter. Unless a designated or approved courier or escort accompanies the material, it will, upon arrival in the recipient country, be delivered to a U.S. Government representative who will arrange for transfer to an authorized representative of the recipient foreign government.

2.31 Receipt System

2.31.1 Top Secret material is transmitted under a continuous chain of signed receipts.

2.31.2 Secret and Confidential material are covered by a receipt between installations and other authorized addressees outside of NASA.

2.31.3 Receipts are provided by the transferring installation, and the forms will be attached or enclosed in the inner envelope or cover. NF 387 will be used for this purpose.

2.31.4 Receipt forms are unclassified and contain only information necessary to identify the material being transmitted.

2.31.5 A duplicate copy of the receipt is retained in a suspense file until the signed original is returned. If a signed receipt is not received within 45 days, follow-up action will be initiated and the cognizant CCPS/CCS will be informed.

2.31.6 Copies of signed receipts will be retained for a period of five years.

2.32 Defense Courier Service Reimbursement Program

Upon request of the AA for Protective Services, the CCPS/CCS shall provide information on the Center's use of the reimbursable service of the Defense Courier Service for transmitting CNSI outside the Center. These costs should also be accounted for annually on the SF 716.

2.33 Disposition or Destruction of Classified Material

2.33.1 Inactive CNSI shall be disposed of in accordance with NPR 1441.1. Each Center will employ security procedures and methods for destruction, witnessing, certification, and retention of CNSI in accordance with this NPR.

2.33.2 Classified information identified for destruction is destroyed to preclude recognition or reconstruction of the classified information.

2.33.3 Centers and other NASA Installations shall continuously review their classified holdings.

Classified information will be destroyed when determined to be no longer required for operational or administrative purposes. The Center CCPS/CCS will establish annual Center-wide classified material destruction events to ensure classified holdings are properly reviewed and unneeded CNSI disposed of in accordance with NPR 1441.1. Prior to any classified information or document being disposed of, the Center Records Manager and the organization that controls the document, in coordination with the Center Protective Services Office, will determine whether the record is a permanent or temporary document, which will determine the disposition of the document. Once the document has been labeled as temporary or permanent, the record will be destroyed or sent to the NASA Records Center or the NARA for storage. Collecting or hoarding CNSI is prohibited.

2.33.4 Additional policy is followed when destroying COMSEC material as contained in NPR 1600.6.

2.33.5 Unclassified material, including formerly classified material that has been declassified and unclassified messages, does not require the same assurances of complete destruction. To avoid overloading an installation's classified material destruction system, unclassified material is introduced only when the CCPS/CCS or higher authority requires it because of unusual security considerations or efficiency.

2.33.6 Approved destruction methods.

2.33.6.1 Only equipment listed on an Evaluated Products List (EPL) issued by the National Security Agency (NSA) may be utilized to destroy classified information using any method covered by an EPL. Only paper-based products are destroyed by pulping. Classified material in microform, that is, microfilm, microfiche, or similar high-data density material, will be destroyed by burning or chemical decomposition or other methods as approved by the cognizant CCPS/CCS. Equipment approved for the destruction of classified material will be operated properly and provided with regular maintenance, as suggested by the manufacturer. The following are the approved methods for the destruction of classified material:

a. Burning. When burning is used for destruction of classified information, ensure that the wind or draft does not carry portions of burned material away and that the resulting ash is broken up sufficiently to preclude reconstruction.

b. Shredding. Any crosscut shredder whose residue particle size is equal to or smaller than 1/32 of an inch in width by 1/2 inch in length (1/32 x 1/2) is approved for the destruction of all classified paper material, magnetic tape, and cards. Do not use shredders to destroy classified microfilm, microfiche, or similar high-information density human readable material. This does not include COMSEC items that are destroyed in accordance with established NSA requirements contained in Committee on National Security Systems (CNSS) Policy No. 16. NSA requirements will be maintained at the Center Security/Protective Services Office.

c. Pulping (Wet Process). Wet process pulpers with a 1/4 inch or smaller security screen will be used to destroy classified water-soluble material. Since pulpers only destroy paper products, staples, paper clips, and other fasteners will be removed to prevent clogging the security screens.

d. Pulverizing (Dry Process). Pulverizers and disintegrators designed for destroying classified material are usually too noisy and dusty for office use, unless installed in a noise- and dust-proof enclosure. Some pulverizers and disintegrators may be used to destroy photographs, film, typewriter ribbons, magnetic tape, flexible diskette (floppy disk), glass slides, and offset printing plates. Pulverizers and disintegrators are required to have a 3/32-inch or smaller security screen.

e. Chemical Process. Classified microfilm or microfiche will be destroyed by chemical process.

2.33.7 Destruction of Classified Equipment.

2.33.7.1 All components of classified equipment will be destroyed by any method that destroys them beyond recognition.

2.33.8 Eradication of Magnetic Media.

2.33.8.1 Destruction of classified Automated Information System magnetic media will be done in accordance with NSA/Central Security Service Policy 9-12 and established NASA COMSEC requirements. A record of destruction will be executed upon eradication of the classified information.

2.33.8.2 The Center Protective Services Office will provide specific guidance on how to destroy newer forms of media as required.

2.34 Destruction Procedures

2.34.1 Classified material will only be destroyed by authorized means by individuals cleared to the level of the material being destroyed. A minimum of two individuals will be responsible for destroying Top Secret material and a minimum of one for Secret and Confidential. These individuals have a need to know and are authorized to destroy the material.

2.34.2 The personnel tasked with the destruction or preparation for destruction of classified material shall be thoroughly familiar with the requirements and procedures for safeguarding classified information. They will be thoroughly briefed on the following:

- a. Safeguarding all classified material entrusted to them for destruction.
- b. Conducting a thorough page check of Top Secret material before destruction is accomplished.
- c. Observing all documents destroyed or being prepared for destruction and checking the residue of locally destroyed material to ensure that destruction is complete and reconstruction is impossible.
- d. Taking precautions to prevent classified material or burning portions of classified material from being carried away by wind or draft.
- e. Completing and signing all appropriate records of destruction.

2.34.3 Classified waste will be destroyed as soon as practicable. Containers used for the accumulation of Secret classified waste will be dated when the first item of classified waste is deposited. If, after 30 days, the classified waste has not been destroyed, a review will be conducted to determine why the information is still being stored and arrangements should be made immediately to destroy the material. When destruction is completed, a record of destruction will be prepared.

2.34.4 The CCPS/CCS shall review or direct a review, at least annually, of Center classified material holdings expressly in order to reduce classified holdings to an absolute minimum.

2.35 Sanctions

2.35.1 NASA Personnel, and its contractors, licensees, certificate holders, and grantees are subject

to appropriate sanctions if they knowingly, willfully, or negligently:

- a. Disclose to unauthorized persons information properly classified under this NPR, E.O. 13526 or predecessor orders and 32 CFR pt. 2001;
- b. Classify or continue the classification of information in violation of this NPR, E.O. 13526 and 32 CFR pt. 2001;
- c. Create or continue a special access program contrary to the requirements of the E.O.; or
- d. Contravene any other provision of this NPR, the E.O. and 32 CFR pt. 2001.

2.35.2 Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanction in accordance with applicable law and NASA policy.

2.35.3 The Administrator or SAO, at a minimum, shall promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in apply the classification standards of this NPR, the E.O. and 32 CFR pt. 2001.

- a. The Administrator or SAO shall;
 - (1) Take appropriate and prompt corrective action when a violation or infraction occurs; and
 - (2) Notify the Director of the Information Security Oversight Office when a violation occurs.

2.36 Security Violations, Security Infractions and Compromise of CNSI

2.36.1 The CCPS/CCS shall ensure that written procedures exist for the following:

- a. Emergency action and reporting requirements for the loss of CNSI.
- b. Action to be taken by the CCPS/CCS in the event of the loss of control over CNSI.
- c. Action required in the event that the lost CNSI was not compromised.
- d. Action required in the event of possible compromise of CNSI.
- e. Action required in the event of unauthorized disclosure of CNSI by NASA personnel.
- f. Documenting unfavorable systemic trends of security violations in order to alert NASA personnel during annual security education.
- g. Notifying the OPS Security Management Division Director, the servicing NASA Counterintelligence office, the Central Adjudication Facility (CAF), and, as appropriate, Center management officials when classified information is presumed compromised.
- h. Notifying the NASA Security Operations Center and Center Chief Information Officer when the incident involves an information system or electronic media as described in ITS-HBK-2810.09-04,
- i. Loss, possible compromise or unauthorized disclosure of classified information or material will be reported immediately to the CCPS/CCS upon discovery of the incident. The CCPS/CCS will appoint a lead from the Center Protective Services Office to head the investigation and to contact the

appropriate organizations required to complete this action. This includes data-spillages on the NASA unclassified network.

2.36.2 A written incident report will be made to the OPS Security Management Division Director on all issues as described in 2.19.1.

2.36.2.1 An initial report of incidents involving classified material requires an immediate notification and presentation of the facts for the purpose of limiting and assessing the damage to the national security. The initial report is due to the OPS Security Management Division Director within two working days. The intent is to notify all critical officials as soon as possible to limit further damage, assess weaknesses, and correct a discrepancy, if appropriate. If a formal report cannot be accomplished in two working days, the OPS Security Management Division Director will be provided with electronic mail that briefly describes the incident, immediate actions taken, and those planned. When a security incident involves the simultaneous compromise of CNSI, sensitive but unclassified information, personally identifiable information (PII), 22 CFR pts. 120-130, 15 CFR pts. 730-774, etc., the Information Security Specialist will take the lead since the CNSI is the highest level of information involved in the incident. A team will be formed consisting of the Center Privacy Manager, ITAR/EAR Manager, and the Center Chief Information Officer Representative to handle and coordinate the other information that falls outside the CNSI arena.

2.36.2.2 Immediate reports of incidents involving classified information will contain the following information:

a. Type of report.

- (1) Compromise.
- (2) Possible compromise.
- (3) Administrative discrepancy.

b. Type of incident:

- (1) Compromise.
- (2) Possible compromise.
- (3) Improper destruction.
- (4) Unauthorized access.
- (5) Improper transmission (transmission via non-secure means or use of unauthorized equipment).
- (6) Improper storage.
- (7) Loss of material.
- (8) Found material (material not in accountability system or previously reported as lost) not subjected to possible compromise.
- (9) Other (explain).

c. Administrative discrepancy:

- (1) Mailed via non-registered/certified mail.

- (2) Sent in single container.
 - (3) Markings on outer container divulged classification of contents.
 - (4) Classification not marked on inner container.
 - (5) No return receipt.
 - (6) Inadequate wrapping: not securely wrapped or protected.
 - (7) Received in poor condition: compromise improbable.
 - (8) Addressed improperly.
 - (9) Classified by unauthorized original classifier.
 - (10) Markings incorrect.
 - (11) Classified by, reason for classification, or declassify on, incorrect or missing (originally classified documents).
 - (12) Derived from or declassify on line incorrect or missing (derivatively classified documents).
 - (13) Other (explain).
- d. Complete identification of all material involved including:
- (1) Unclassified title.
 - (2) Classification.
 - (3) Originator.
- e. Identity of all personnel involved including:
- (1) Full name.
 - (2) Social Security Number.
 - (3) Security Clearance.
 - (4) Basis of Security Clearance.
- f. A statement of actions taken upon discovery of incident and description of events.
- g. Weakness leading to the incident.
- h. Corrective actions taken and actions taken to preclude recurrence.
- i. Disciplinary action taken, if any.
- j. Unit incident number, to include:
- (1) Fiscal year.
 - (2) Sequential number.

2.36.3 The CCPS/CCS shall submit a final incident report within 30 days of the incident. The report

will include:

- a. Likelihood CNSI was compromised (provide details supporting determination).
- b. General comments (may include authority to remove material from accountability or request further information).
- c. Incident closure or further investigation required.
- d. Center incident number (to include fiscal year and sequential number).

2.36.4 The CCPS/CCS shall track security infractions to identify systemic trends. Security infractions are administrative errors that do not result in the compromise of CNSI. Unfavorable systemic trends will be addressed in annual security education training and with remedial training for repeat offenders.

2.36.5 The Office of Protective Services will report all security violations and corrective actions to ISOO.

2.37 CNSI Meetings

2.37.1 Any meeting (conference, seminar, symposium or exhibit) sponsored by NASA or held at a NASA Center where classified information is disclosed will meet the minimum-security standards established in paragraph 2.20.3 and be coordinated by the Center OPS.

2.37.2 NASA may host meetings held by an association, society, or other group whose membership consists of cleared personnel. The membership and NASA CCPS/CCS will ensure the following:

- a. An authorized contract is in place.
- b. An appropriately trained clearance holder is designated and responsible for furnishing all security measures for the meeting.

2.37.3 The Center OPS shall request approval from the OPS SMD approval for a NASA-sponsored meeting involving CNSI discussion and presentations. The request will include an event security plan detailing physical and industrial security procedures to be enforced.

2.37.4 The OPS SMD shall approve classified meetings requiring foreign national or foreign representative attendance in accordance with NPR 1600.4.

2.37.5 The CCPS/CCS shall ensure the following minimum security standards are met:

- a. A classified meeting is restricted to appropriate areas at Government or contractor facilities approved for classified discussions.
- b. Supervisors and meeting hosts shall ensure that all attendees possess the appropriate personnel security clearances and a need-to-know.
- c. A request for security approval for a CNSI meeting is forwarded through the CCPS/CCS to the OPS Security Management Division Director. The request will include the following items: date(s) and specific location for the proposed meeting (Government or cleared contractor facility), identification of CNSI subject matter and highest classification level involved, and the identification and status of any non-U.S. citizen (Foreign National or resident alien) and foreign representative

invited to attend during any classified or unclassified session.

d. If any non-U.S. citizen or foreign representative is in attendance, the following information will be submitted to OPS SMD: complete name, date, place of birth, current citizenship status, type of personnel security clearance (if any), identification of each foreign government and/or entity represented, date(s) of attendance, nature of participation, and the reason why attendance is considered to be in the U.S. national interest.

e. Foreign nationals or foreign representatives will not be invited to attend or permitted to attend any classified meetings unless advance approval has been obtained from the OPS SMD. Refer to NPR 1600.4 for more detailed requirements on facilitating foreign national visits.

f. The CCPS/CCS or staff shall implement necessary security measures; conduct a visual and physical inspection of the meeting room to help preclude any unauthorized disclosures of classified information.

2.38 Security Areas

2.38.1 Requests for collateral-level secure vault areas/conference rooms are submitted to the CCPS/CCS for approval and are constructed to meet Intelligence Community Directive (ICD) 705. At a minimum, these areas are designated "Limited Areas."

2.38.2 Requests for unattended open storage areas containing collateral-level Confidential or Secret level CNSI materials are submitted to the CCPS/CCS for approval. Approval can only be granted when construction standards meet ICD 705. These areas are designated "Exclusion Areas."

2.38.3 Requests for open storage areas containing collateral-level Top Secret level materials are submitted to OPS SMD for review and approval. Approval can only be granted when construction standards meet ICD 705. These areas are designated "Exclusion Areas."

2.39 Classified Material Ownership

2.39.1 Classified information is always official U.S. Government information and never personal property of the individual. Confusion sometimes arises about classified notes from a training course or conference. Classified material is official U.S. government property that will be safeguarded, transmitted, and destroyed in accordance with this NPR. Classified notes cannot be removed from a NASA installation without the approval of the Center Director or CCPS/CCS. Classified notes are not working papers but official information for which the Center/facility is responsible. Classified notes are transmitted by one of the authorized transmittal methods for classified material. When an individual leaves one NASA installation and transfers to another, the installation may officially transfer his/her notes as classified material to the new NASA installation where the material will again be available for his/her use. If the individual desires to have material transferred to another U.S. Government agency, the CCPS/CCS will facilitate the transfer of physical information. However, CCPS/CCS will inform OPS, SMD to facilitate technology transfers. Derivative classifiers may share information with other U.S. Government agencies if they have met the requirements outlined in 2.7 of this NPR.

2.39.2 CNSI is always the property of the United States Government. Individuals who remove CNSI without proper authorization may be subject to disciplinary action up to and including criminal

prosecution under Titles 18 and 50 of the United States Code and other applicable laws.

2.40 Security Classification Reviews for NASA Programs and Projects

2.40.1 Pursuant to NPR 7120.5, NPR 7120.7, and NPR 7120.8, programs and projects conduct formal security reviews that, in addition to personnel, physical, and information technology security, include reviews for traditional information classification security needs. Security reviews will be undertaken to determine if information used or produced as part of a program or project, meets the requirements for designation as CNSI controlled information. Program and project managers will contact their local Center Protective Services Office for classification assistance at the beginning of all new projects as required. Project managers will:

- a. Complete NF 1733. The local Center Security Protective Services Office Information Security Specialist should be consulted for assistance with this form and the classification process.
- b. Take the completed form to the Center Protective Services Office for review and approval.
- c. Include the NF 1733 as permanent program documentation and in any procurement-related documentation.

2.40.2 Upon the conclusion of the security review, if the information surrounding or concerning the program or project, or portions thereof, meet one or more of the categories of information presented in E.O. 13526, a subject matter expert (SME) with assistance from OPS and the CCPS/CCS, as appropriate, develops an appropriate SCG. The SME and project officials shall consider the level of classification needed for specific information. APPENDIX A provides a definition of each. SMEs specifically identify what particular information is under consideration for classification. The SME will provide a recommendation of the classification level (Top Secret, Secret, or Confidential) and duration of protection to OPS. The “NASA Handbook for Writing Security Classification Guides” formally prescribes information that is contained in an SCG and can be obtained from the OPS Information Security Program Manager. Duration of classification will be considered within the following guidelines:

- a. The SME shall attempt to determine a date or event that is less than 10 years from the date of original classification and that coincides with the lapse of the information’s national security sensitivity and will assign such date or event as the declassification instruction.
- b. If unable to determine a date or event of less than 10 years, the SME shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision.
- c. If unable to determine a date or event of 10 years, the SME shall assign the declassification date not to exceed 25 years from the date of the original classification decision.

2.40.3 All SCGs are approved by OPS. The CCPS/CCS and the OPS Security SMD shall assist program and project managers in the development of SCGs. All SCGs are signed by a NASA OCA with Technical Concurrence from the Associate Administrator for the appropriate Mission Directorate.

2.40.4 The OPS will establish and maintain a central repository for all NASA-originated SCGs and declassification guides. The OPS will also obtain and maintain SCGs and declassification guides from other Agency programs in which NASA is working or supporting. The CCPS/CCS will ensure

the OPS Security Management Division Director has the most recent version of program SCGs for their Center.

Pursuant to 32 CFR 2001.16 and section 2.42.1.d. of this NPR, the CCPS/CCS will conduct a fundamental classification review of NASA SCGs every 5 years by for SCGs under their Center. The fundamental classification review focuses on:

a. Evaluation of content.

(1) Determining if the guidance conforms to current operational and technical circumstances.

(2) Determining if the guidance still meets the standards for classification under section 1.4 of the E.O. and the assessment of likely damage under section 1.2 of the E.O.

b. Evaluation of use.

(1) Determining if the dissemination and availability of the guidance is appropriate, timely, and effective.

(2) An examination of recent classification decisions to ensure that classification decisions reflect the intent of the guidance as to what is classified, the appropriate level, the duration, and associated markings.

2.40.5 Upon completion, termination, or cancellation of a program or project, a declassification guide is produced to provide the necessary requirements for declassifying the project information. The declassification guide is approved by the OPS. 32 CFR 2001.32 contains additional details pertaining to declassification guides.

2.40.6 If information surrounding or concerning the program or project is considered unclassified, a letter of transmittal is produced that reflects this determination. The project office will maintain the original letter with copies sent to the appropriate responsible Mission Directorate and to the OPS Security Management Division Director.

2.40.7 All CNSI information should be reviewed by a records manager, the responsible program manager/office head, and a Declassification Authority (DCA), if the information is classified, to determine the disposition of the records before they are sent to the Federal Records Centers or the NARA for temporary or permanent storage.

2.41 Access to Classified National Security Information Granted by Another Government Agency

2.41.1 All NASA employees receiving access to classified information from other government agencies such as the Department of Energy, Department of Defense, National Security Agency, Department of Homeland Security, Nuclear Regulatory Agency, State Department or any other Government agency shall protect and control the classified information in accordance with the regulations and policies provided to them by the agency granting the access and need to know. The employee will contact their NASA Center Protective Service Office to receive assistance with safeguarding and protecting the information if they are required to maintain the classified information at a NASA Center, Component Facility, or location.

2.41.2 CCPS/CCS shall report to OPS, SMD all other government programs performed at their

Center and ensure that Center employees are properly handling and safeguarding other government classified information.

2.42 Special Access Program (SAP)

2.42.1 A SAP may be created within NASA only upon specific written approval of the Administrator and coordinated with the Office of Protective Service Intelligence Division Director to ensure required security protocols are implemented and maintained. The Administrator, along with SAO and the Office of Protective Services Intelligence Division Director, reviews each SAP annually to determine whether it continues to meet the requirements of E.O. 13526.

2.42.2 All personnel security requirements for NASA personnel to establish and participate in SAP external to NASA is coordinated with the OPS Intelligence Division Director to ensure accountability of NASA equities.

2.42.3 All NASA security activity associated with SAPs are authorized and prescribed by the NASA Special Access Program Security Guide (SAPSG). All NASA SAPs will adhere to the standards in the SAPSG. Other Federal Agency SAPs supported at NASA facilities will adhere to the NASA SAPSG when there is no policy or direction provided from the other agencies.

2.43 Information Systems (IS)

2.43.1 Information systems (IS) that are used to capture, create, store, process, or distribute CNSI will be properly managed to protect against unauthorized disclosure of classified information, loss of data integrity, and to ensure the availability of the data and system. OPS shall be responsible for the certification and accreditation for all NASA National Security Systems, networks, and Protected Distribution Systems.

2.43.2 Protection requires a balanced approach, including information systems security features to include, but are not limited to, administrative, operational, physical, computer, communications, and personnel controls. Protective measures commensurate with the classification of the information, the threat, and the operational requirements associated with the environment of the information systems are required. Information will not be downloaded onto memory sticks, jump drives, USB flash drives, or any other type of device without specific documented approval from the information system owner or the authorized security official that controls access to the system.

2.43.3 The CCPS/CCS will submit the request for Authorization to Operate (ATO) to the Office of Protective Service Authorizing Official (AO) at HQ for approval.

2.43.4 The CCPS/CCS shall follow the National Institute of Standards and Technology (NIST) Risk Management Framework when establishing information systems and networks that access, process, store, or transmit CNSI. The CCPS/CCS will ensure that the information system is secured in accordance with the Committee on National Security Systems (CNSS) Instruction 1253, NIST Special Publication 800-53, and NIST Special Publication 800-37.

2.44 ISOO Reporting Requirements

2.44.1 OPS is responsible for compiling data received from CCPS/CCS and completing the

following annual reports to ISOO in accordance with E.O. 13526 and 32 CFR pt. 2001:

a. ISOO SF 311.

b. ISOO SF 716. The CCPS/CCS will work with the appropriate personnel to ensure that the best estimates are collected for inclusion on the Annual ISOO Cost Estimates for Security Classification Activities for each fiscal year. The cost estimates will be incorporated and consolidated into the Agency's external reporting requirement to ISOO as described in Section 2.42 of this NPR. The costs estimates reported to the OPS Security Management Division Director on the SF 716 will only be associated with the protection of classified information, not security costs for the protection of property or unclassified information. The following categories will be included:

(1) Personnel Security.

(2) Physical Security.

(3) Classification Management.

(4) Declassification.

(5) Protection and Maintenance for Classified Information Systems.

(6) Operations Security and Technical Surveillance Countermeasures.

(7) Professional Education, Training and Awareness.

(8) Security Management, Oversight and Planning; and

(9) Unique Items.

c. ISOO Senior Official Self-Inspection Program Report.

d. Fundamental Classification Guidance Review.

e. Security Violations and Sanctions. In accordance with Section 5.5 of E.O. 13526 and 32 CFR pts. 2001.48(d) & 2001.91(d), the OPS will report to ISOO any violation or sanction that is prohibited by the E.O. that:

(1) Is reported to oversight committees in the Legislative branch;

(2) May attract significant public attention;

(3) Involves large amounts of classified information; or

(4) Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

2.45 Self-Inspections

2.45.1 The CCS/CCPS will conduct internal self-inspections at least once annually and report the results to OPS, SMD Information Security Program Manager.

a. The internal annual self-inspection program will be documented and maintained for a period of three (3) years. The internal annual self-inspection includes evaluation and effectiveness of Center programs covering:

- (1) Original classification.
 - (2) Derivative classification.
 - (3) Declassification.
 - (4) Safeguarding (to include telecommunications, automated information systems, and network security).
 - (5) Security violations and security infractions.
 - (6) Security education and training.
 - (7) Management and oversight of internal self-inspections.
 - (8) Include regular reviews of representative samples of Centers' original (where applicable) and derivative classification actions; these samples will encompass all Center activities that generate classified information and evaluate the appropriateness of classification and proper application of document markings. This review will also include interviews with personnel that produce and use classified and classified electronic records pursuant to 32 CFR pt. 2001.
- b. Center self-inspection programs will use the Agency Self-Inspection Program Data form to facilitate the annual ISOO reporting requirement. The Agency Self-Inspection Program Data form will be completed and reported annually to the OPS Security Management Division Information Security Program Manager for incorporation and consolidation of the Agency's external reporting requirement to ISOO.
- c. The CCPS/CCS shall conduct regular and periodic reviews of NASA organizational units involved in original (where applicable) and derivative classification, storage, and processing of classified material under the jurisdiction and custody of their respective Center, to ensure compliance with E.O. 13526, 32 CFR, pt. 2001, this NPR, and any applicable local procedures.
- (1) Reviews will meet the intent of 32 CFR pt. 2001 and be reported annually to the OPS Security Management Division Information Security Program Manager on SF 311. The annual SF 311 form is not an audit and is used to report all classification decisions (declassification, original and derivative actions), inspections, and other classification management statistics at the Center. As with the Center Self-Inspections, classification management statistics will also include classified electronic records pursuant to 32 CFR § 2001.23.

Chapter 3. Sensitive Compartmented Information Programs

3.1 General

3.1.1 The requirements detailed in this chapter are in addition to the CNSI requirements detailed in the previous chapter.

3.1.2 Procedures. The policies, procedures, and responsibilities outlined herein supersede all prior NASA SCI security program documents and policies of a similar kind, excepting those contained in NPR 1600.1, NPD 1600.4, this NPR, and all applicable national-level policies and procedures regarding SCI clearances and SCI Programs, including, but not limited to, all Cognizant Security Authority (CSA) and Office of the Director of National Intelligence (ODNI) directives.

3.1.3 Special Security Program. The NASA SCI program is designated as a Special Security Program. The Agency SSO/Intelligence Division Director or their designee(s) will regularly review current threat assessments detailing the criminal, espionage, sabotage, subversion, and terrorist threat environment from NASA's Counterintelligence/Counterterrorism Division or law enforcement entity. Risk management-based countermeasures will be implemented accordingly against these threats.

3.1.4 Special Security Position Appointments. Each NASA Center Chief of Protective Services (CCPS) or their designee, or for NASA Headquarters, the Agency SSO/Intelligence Division Director or their designee, will appoint an SSO, Special Security Representative (SSR), or Assistant Special Security Officer (ASSO), in writing, and establish procedures for SCI indoctrinated personnel to communicate directly with their respective SSO concerning all SCI security related matters.

3.1.5 Public Disclosure of Classified Information. Information classified as SCI will not be published, released, or discussed with unauthorized persons, including the public media. Declassification of SCI for public release is not authorized without the prior written approval of the appropriate security executive agent. Requests for such declassification action will be forwarded through the Agency SSO/Intelligence Division Director.

3.1.6 The Assistant Administrator for Protective Services (AA, OPS) is responsible for the following:

- a. Developing, coordinating, and promulgating all NASA national security program policies.
- b. Directing the Director, Intelligence Division to administer the SCI security program for NASA and to serve as the Agency SSO.

3.1.7 The Agency SSO/ Intelligence Division Director (Hereafter referred to as the Agency SSO) is responsible for the following:

- a. Administering security for the SCI program for NASA.
- b. Serving as NASA's representative to the United States Intelligence Community for all matters relating to NASA SCI security operations.

- c. Advising the AA, OPS and agency leadership on agency-wide security for SCI operations.
- d. Administering SCI governance security policies and procedures consistent with that of appropriate executive agents in the protection of National Security.
- e. Retaining security cognizance over all NASA Center SCI programs, including Sensitive Compartmented Information Facilities (SCIFs).
- f. Providing SCI security program oversight, direction, and guidance to all NASA Centers on SCI operations.
- g. Notifying the Director of CI for Protective Services about any loss, compromise, or suspected compromise of SCI materials.
- h. Administering uniform NASA SCI policy in accordance with established regulations and mandates on the interrelated disciplines of:
 - (1) Information Security (INFOSEC).
 - (2) Personnel Security (PERSEC).
 - (3) Physical Security.
 - (4) Technical Security - TEMPEST and Technical Surveillance Counter-Measures (TSCM).
 - (5) Information Systems Security.
 - (6) Security Education, Training, and Awareness (SETA).
 - (7) Industrial Security – contractor SCI program administration.
- i. Developing and overseeing a program that ensures NASA's compliance with SCI program requirements by performing reviews in accordance with NPD 1210.2.
 - (1) Reviewing all administrative actions relating to the Center's SCI security program, including, but not limited to the following:
 - (a) Annual self-inspections.
 - (b) SETA material.
 - (c) PERSEC files.
 - (d) Administrative waivers.
 - (2) Providing a written report detailing the results of each inspection to the applicable Center Director with the following:
 - (a) All identified vulnerabilities.
 - (b) Corresponding corrective actions.
 - (c) A suspense date to complete all corrective actions and/or a request for the appropriate waivers.
- j. The establishment of new SCIFs and SCIF modifications within NASA.

k. Ensuring all Scattered Castles data is accurate and submitted in a timely manner, to include: (1) A total records refresh is performed at least once every 30 days.

(2) Records, including briefings and debriefings, are updated at least weekly.

(3) All clearance denials, revocations, and suspensions are recorded within 24 hours of the decision.

k. The establishment of a standardized NASA SCI SETA program.

l. The establishment of an Agency-wide annual SCI self-inspection program.

m. Maintaining physical security and TEMPEST accreditations for NASA Centers and NASA contractors, as required.

n. Reviewing and providing concurrence on all SCI briefing materials relating to SCI indoctrination, debriefing, and execution of applicable Non-Disclosure Agreements (NDA) for NASA Centers.

3.1.8 The Center SSOs are responsible for the following:

a. The application and maintenance of Standard Operating Procedures (SOP) regarding NASA's SCI security program.

b. Overseeing all administrative elements, as required, in accordance with National, Agency, and local policies and procedures.

c. Implementation of NASA's SETA Program.

d. Ensuring all information, logical and in hard-copy form, relating to SCI security programs (PERSEC, physical security, INFOSEC, etc.) is properly maintained within an accredited SCIF.

e. Ensuring when using a contractor SSR that they are on a valid contract with the appropriate accesses authorized by a DD Form 254, Contract Security Classification Specification.

f. The duties of a SSR will be placed within the applicable performance work statement to ensure the appropriate knowledge, skills, and abilities are in place to meet the needs of the Center.

3.1.9 Center Directors or Officials-in-Charge (OIC), regardless of whether there is a SCIF at their Center, will appoint a civil servant SSO, in writing, to serve as the Center point-of-contact concerning all matters relating to SCI security and to administer National policy and directives (e.g. Intelligence Community Directives), as well as applicable NPRs, for their respective Centers. The designated SSO will have a requisite SCI clearance.

3.1.10 Special Security Representatives (SSR) and Assistant Special Security Officer (ASSO). The CCPS/CCS or their designee, or for Headquarters, the Agency SSO or their designee, may also appoint an SSR and/or ASSO to operate under the direction of the SSO to support day-to-day management and implementation of SCI security and administrative instructions for the SCI program located at that Center or at Headquarters. SSRs and ASSOs can be either civil servants or contractor, but will have the required skills, training, and experience to fulfill the specified duties.

3.2 Information Systems for processing SCI information

3.2.1 It is the responsibility of each Center SSO to coordinate with the NASA National Security Systems (NSS) Team to ensure that documentation for information systems residing within their

SCIF(s) is compliant with ICD 503/NIST 800-53 requirements.

3.2.2 The NASA NSS Team is responsible for the development and accreditation of classified information systems used in support of NASA SCI programs.

3.2.3 The NASA NSS Team develops and maintains an accreditation/certification support documentation package for system(s) for all Centers.

3.2.4 The Center SSO will approve all information systems and components prior to their physical introduction into a SCIF.

3.2.5 The Center SSOs and NASA NSS Team personnel will ensure systems are operated, maintained, and disposed of in accordance with ICD 503/NIST 800-53.

3.3 Self-Inspections of the SCI Program

3.3.1 Center SSOs will conduct, at a minimum, annual self-inspections of their SCIF space.

3.3.2 SCIF self-inspections will utilize the Fixed Facility Checklist, to the extent possible, along with any self-inspection checklist approved by the Agency SSO.

3.3.3 Self-inspection findings will be provided in writing to the applicable CCPS/CCS and the Agency SSO by the Center SSO.

3.3.4 Functional Inspections.

3.3.4.1 A full inspection including a thorough review of all functional areas involving Center SCI security programs (e.g. security administration, information security, personnel security, physical security, technical security such as TEMPEST and TSCM, security education, information systems security, and other requirements outlined in this appendix) will be conducted by the AA, OPS or their designee as part of the Center's functional review.

3.3.4.2 The functional inspection of the Center's SCI security program will ensure compliance with the policies and procedures contained in this appendix and other applicable policy, regulations and directives.

3.3.5 Other Inspections.

3.3.5.1 The Agency SSO and/or their designee is authorized to conduct inspections as needed. Inspections will be announced by the Agency SSO unless they are aware of critical information requiring immediate remediation to prevent the likely unauthorized disclosure of SCI information.

3.3.5.2 Introduction of inspection equipment into a SCIF will be coordinated with the Center SSO prior to a site visit.

3.3.5.3 Periodic inspections may be scheduled based on threat, sensitivity, physical modifications, and past security performance.

3.3.5.4 Additional inspections may be conducted in the event of suspected compromise, loss of information, history of deficiencies, major facility modification, or change in threat level.

3.3.5.5 Inspectors will submit a written report following each inspection identifying any deficiencies and corrective action to be taken.

- a. The report will be forwarded to appropriate CSA officials upon request.
 - b. All copies will be maintained within the inspected SCIF and by the Agency SSO and/or their designee.
- 3.3.5.6 Joint agency tenants of the SCIF will accept the results of CSA security reviews for validation of security compliance.
- 3.3.6 All written reports will be available to the ODNI or designee upon request.

3.4 Facility Accreditations

Centers shall request the Agency SSO conduct a site survey prior to requesting SCIF accreditation by the CSA.

3.5 Contractors performing SCI

- 3.5.1 Contractors performing SCI work at NASA Centers shall have a DD Form 254 incorporated in their NASA classified contract, per NASA FAR Supplement subpt. 1804.4.
- a. The DD Form 254 provides the contractor (or a subcontractor) with security requirements and the classification guidance necessary to perform on a classified contract. Center SSOs shall indicate the appropriate clearance and access levels required on the DD Form 254.
 - b. The Center SSO shall validate the contractor company's Facility Security Clearance (FCL) level and current status of contract prior to processing a contractor for SCI access.
- 3.5.2 Contractors shall ensure SCI information in their custody at the Center is used or retained only in furtherance of a lawful and authorized U.S. Government purpose.
- 3.5.3 Contractors are not permitted to remove any SCI material from their respective Center SSO when their contract expires or closes out unless the U.S. Government has given the contractor expressed permission to retain classified material in accordance with current directives. If requested, this requirement will be included in item 13 or 14 of the DD Form 254.

3.6 Standard Classification Markings

- 3.6.1 Classification and control markings will be applied explicitly and uniformly when creating, disseminating, and using classified and unclassified information to maximize information sharing while protecting sources, methods, and activities from unauthorized or unintentional disclosure.
- 3.6.2 Documents containing SCI will be marked in accordance with the Intelligence Community Authorized Classification and Control Markings Register and Manual (CAPCO Register) issued by the Office of the Director of National Intelligence, Controlled Access Program Coordination Office.
- 3.6.3 Standard classification markings indicate the level of classification, the source of classification decisions and the agency and office of origin ("Classified by"), the reason for classification ("Reason"), and downgrading and declassification instructions ("Declassify on").
- 3.6.4 Warnings notices (if applicable), intelligence control markings, portion markings, and page

markings will be included in accordance with the CAPCO Register.

3.7 Storage

3.7.1 Storage of SCI material will be maintained and stored in an accredited SCIF, in accordance with the respective SCIF's accreditation.

3.7.2 U.S. collateral classified information used in a SCIF will be stored in accordance with the SCIF accreditation.

3.8 SCI Accountability

3.8.1 Material specifically designated by the IC or the Agency SSO, as accountable SCI will employ document numbers and other similar systems to provide accountability.

3.8.2 Refer to the respective SCIF SOP for additional procedures.

3.9 Media

3.9.1 All individuals requiring access to classified information systems will meet the following requirements prior to establishing accounts:

- a. Complete the annual security training for clearance holders.
- b. Coordinate approval through the Center COMSEC Officer, Center SSO, NASA NSS Team, and authorized approver at the discretion of the Center Director or designee.

3.9.2 The introduction and removal of media and/or hardware from a SCIF will be in accordance with document control procedures established by the Center SSO.

3.9.3 Each media item (e.g. CDs, DVDs, hard disk drives, etc.) brought into the SCIF will be externally labeled and controlled.

3.9.4 The Center SSO, in coordination with the NASA NSS Team, will maintain an inventory of all IS hardware resident within the SCIF.

3.10 Document Control Procedures

3.10.1 SCI material will not be sent to a facility that does not have a SCIF, to an individual who is not SCI accessed, or does not have access to a SCIF.

3.10.2 All SCI materials will be properly marked and, when required, have cover sheets attached.

3.10.3 Any loss, compromise, or suspected compromise of SCI materials will be immediately reported to the Center SSO and to the Agency SSO.

3.11 Transportation of SCI

3.11.1 The preferred method of transporting SCI from one SCIF to another is via secure e-mail or

other secure electronic means. Alternatively, SCI may be transported by SCI-indoctrinated persons or certified/designated couriers.

3.11.2 SCI materials sent between SCIFs within a Center will be hand carried by individuals who are properly briefed on courier procedures, possess a valid courier card or letter, and who are cleared to the same level as the material being transported.

3.11.3 The Center SSO will establish accountability and control for courier cards and authorization letters, in accordance with established regulations.

3.11.4 Transporting SCI materials within a single building or between two different locations will be done in accordance with national policies governing the transportation of SCI information.

3.12 Electronic Transmissions

3.12.1 All SCI transmissions will be conducted in accordance with current IC policies.

3.12.2 SCI will be processed only on a computer, or network of computers, that has been specifically certified and accredited for that level of classified information in an accredited location. Additionally, SCI materials may be electronically transferred between appropriately accredited machines (facsimile, computers, secure voice, secure e-mail, or any other means of telecommunication ensuring that such transmissions are made only to authorized recipients). It is essential to ensure that appropriate secure devices are used for any electronic transfer of SCI material.

3.12.3 Multi-Function Office Machines are devices that have the capability to copy, print, scan, and fax, either in a standalone or networked mode. When connected to a network, these devices assume the highest classification for which the network is accredited and will be labeled as such. If operated as a standalone or multi-function device, these devices assume the highest classification of copied documents and will be labeled with the highest classification level. Many of these devices have hard drives capable of holding thousands of images depending on the size and complexity of the images. The SSO will establish written procedures to protect the information contained within the hard drive and printed circuit boards/memory boards of these devices.

3.12.4 Reproduction. The SSO will establish procedures to ensure reproduction of SCI documents are consistent with operational necessity to ensure accountability and reduce the potential for an insider threat incident. The SSO will establish procedures for annual classified holdings retention review. Copies of documents are subject to the same control, accountability, and destruction procedures as the original documents. Extracts of documents will be marked according to content and treated as working materials.

3.12.5 Disposition General Provisions. Classified information no longer needed will be processed for appropriate disposition and destroyed in accordance with security standards governing the disposition of SCI.

3.13 Emergency Plans

3.13.1 Plans will be developed in coordination with the appropriate NASA Continuity of Operations (COOP) representative to protect, remove, or destroy classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or any other emergency situation.

3.13.2 The Center SSO or designated SCI-indoctrinated individuals will handle classified material according to their emergency plan during an emergency, unless in the case of extenuating circumstances, while minimizing any risk to the greatest extent possible.

3.14 Request for SCI Access

3.14.1 Determinations for individuals to obtain and retain access to classified information will be made with consideration of national security and, thus, granted accordingly.

3.14.2 The granting of access to SCI will be controlled under the strictest application of the “need-to-know” principle and in accordance with personnel security standards and procedures.

3.14.3 Positions that require access to SCI will be designated as “Special-Sensitive” and reflected in the NASA employee’s position description, as established in accordance with the procedures of the Office of Human Capital Management.

a. If TS/SCI access is requested but is not yet included in the employee position description, a completed SAR Form 2018a is submitted to the AA, OPS to waive this requirement until the employee’s position description is updated to reflect the designation.

3.14.4 Contractors requiring access to SCI shall be assigned to a valid contract with the appropriate accesses authorized by their DD Form 254.

3.14.5 A Tier 5 background investigation will be conducted on individuals under consideration for initial or continued access to SCI.

3.14.6 NASA’s Central Adjudication Facility (CAF) determines the Top Secret eligibility for civil service employees requiring access to SCI and is responsible for compiling and submitting the required documents for CSA approval. They will also facilitate the requests through final adjudication. When required for the adjudication process, the CAF will contact the appropriate Center Protective Services Office if any additional information is needed.

3.14.7 SCI requests for contractor personnel will also be processed by the CAF.

3.14.8 Evaluation of the information developed by investigation regarding an individual’s loyalty and suitability for SCI access will be conducted by the CSA.

3.14.9 CSA approval timeframes depend on backlog and composition of access requests. Additional documents or other information may be required at the request of the CSA.

3.15 Reporting Requirements

3.15.1 SCI access for all NASA employees and contractors is granted exclusively by the CSA. As a condition for continued SCI access, NASA SCI clearance holders are required to follow all current CSA and ODNI reporting requirements and regulations. NASA policy or procedure does not supersede CSA and ODNI directives or policies.

3.15.2 Foreign contacts. Foreign contacts as defined in the ODNI Security Executive Agent Directive 3 (SEAD 3) will be reported to the Center SSO and CSA or their designee(s) via NASA reporting mechanism.

3.15.3 Foreign contact information will be provided by NASA employees and contractors to the Center SSO in a timely manner. The Center SSO will forward foreign contacts and other required reporting information to NASA's CAF when received.

3.15.4 Foreign travel. Advance written notice will be provided to the CSA or their designee(s) for persons currently approved or applying for SCI access who anticipate or plan any travel, whether official or unofficial, to or through, or who are being assigned to duty in, foreign countries and areas, except as noted in current CSA and ODNI directives and policies. This includes those with pending indoctrination. All unofficial travel will be reported through the NASA Foreign Travel Reporting Tool. An automated travel notification, via the NASA foreign travel reporting tool, will be provided to the NASA CAF, and NASA Counterintelligence Office (CI) to receive appropriate defensive security briefings prior to travel.

3.15.5 When traveling to a foreign designated country or Russia, notify the servicing NASA CI office to receive appropriate defensive CI and counterterrorism briefing prior to travel.

3.15.6 Clearance holders shall report any suspicious activity experienced the foreign travel to the Center SSO and the NASA CI office.

3.15.7 Foreign and Suspicious Activities. Any suspicious activities as defined and detailed in SEAD 3 and other current ODNI directives and policies will be reported by NASA employees and contractors to the Center SSO in a timely manner. The Center SSO will forward the foreign activities information to the NASA CAF. The NASA CAF will report relevant information to the CSA.

3.15.8 Reportable Actions by Others. In accordance with current ODNI directives and policies, individuals observing suspicious actions or specific behaviors incongruent with standards for those having SCI access will be reported to the servicing NASA CI office and/or NASA Insider Threat Program, per NPD 1600.9, for further evaluation.

3.16 SCIF Construction Procedures

3.16.1 Documents pertaining to SCIF construction will be submitted to the Agency SSO or their designee(s) via an approved system. This pertains to either new facility construction or modification to an accredited facility.

3.16.2 Pre-Construction. At a minimum, the following will be submitted to the Agency SSO or their designee(s) prior to the Initial Site Survey and construction:

- a. SCIF justification approval request
- b. Construction Security Plan
- c. Fixed Facility Checklist
- d. Initial drawings
- e. TEMPEST Checklist

3.16.3 Mid-Construction. Additional information may be requested by the CSA during any phase of construction (e.g. updated drawing, photos, etc) and should be submitted in a timely manner to the Agency SSO or their designee(s).

3.16.4 Final Accreditation. Prior to final accreditation of the facility, in addition to any updates to required documents, the SOP and an Emergency Action Plan will be submitted for approval.

3.17 Co-Use Agreements

Any use agreements regarding NASA SCIFs (e.g. MOU, MOA, etc.) will be coordinated through the Agency SSO or their designee(s). This includes both program and agency agreements.

3.18 SCI File Transmission Procedures

3.18.1 Documents will be sent in accordance with directives regarding transmissions based on classification and sensitivity. The following documents should be sent electronically:

- a. Personnel Security documents
- b. CSA additional information responses
- c. Physical Security documents
 - (1) Documents, including photos pertaining to new or reaccreditation of SCIFs;
 - (2) Co-Use Agreements
 - (3) MOUs
 - (4) Waivers
- d. Information regarding account access.
- e. Matters pertaining to Public Key Infrastructure (PKI).

3.19 SCI Visit Requests

3.19.1 NASA personnel seeking to have their clearances passed to other federal agencies or contractor facilities where SCI access is required will complete NF 1833 under the terms of either a Visit Authorization Request (VAR) or Perm Cert as defined below, and submit it to the Center SSO.

- a. Visit Authorization Requests (aka Term Cert) - Visits authorized for a period of less than 90 days.
- b. Perm Certs—Visits authorized for a period greater than 90 days and not to exceed 12 months under the following terms and conditions:
 - (1) Requestor visits the agency/facility regularly with the first visit occurring within 30 days of the submission of the request.
 - (2) SSO will maintain a record-keeping capability, preferably electronic, for tracking Perm Cert expiration dates and make appropriate notifications to Perm Cert holders of impending expirations 30 days prior to actual expiration dates.

3.19.2 It is the responsibility of the requesting individual to obtain the necessary information from their point of contact required to complete the NF 1833.

3.19.3 Using the information obtained in NF 1833, the Center SSO will prepare and transmit a VAR or Perm Cert in the manner preferred by the receiving security office. This may include the use of NASA letterhead or Center-specific VAR form that contains all the necessary clearance and personal identification information required by the receiving SSO at the site to be visited. Acceptable methods of transmission may include the use of an unclassified email (encrypted to protect personal identifying information), email on SCI-level network, classified fax, or unclassified fax.

3.19.4 Visit Requests and Perm Certs records will be retained for a period of five years. Center SSOs will provide the Agency SSO details regarding all clearances passed.

3.19.5 Visitors to NASA SCIFs. Visitors from external agencies requesting access to NASA SCIFs will use the VAR and Perm Cert validity time-frame standards of less than 90 days for VARs and greater than 90 days for Perm Certs. VARs and Perm Certs should be submitted to the respective NASA Center SSO at least five working days prior to their arrival whenever possible.

Note: A VAR is not required when the NASA POC sponsoring the visit supplies the names, social security numbers, and government or contractor affiliations sufficient to validate each visitor in Scattered Castles or determine that a formal VAR is required otherwise.

a. Verification of clearance and access for all visitors may be accomplished through either of the methods below:

(1) Scattered Castles. The Scattered Castles database is the authoritative source for personnel security access approval verifications regarding SCI and other controlled access programs, visit certifications, and documented exceptions to personnel security standards.

(2) VAR or Perm Certs sent from the visiting agency if security clearances/accesses cannot be validated in Scattered Castles.

b. If clearances/accesses are not found or shown to be active in Scattered Castles for non-NASA affiliated contractors visiting NASA SCIFs, their VAR or Perm Cert requests will be submitted to NASA via their government sponsoring agency by any of these methods: electronic transmission, visit requests in the format generated by security management applications, or on organizational letterhead to the respective Center SSO with cognizance over that specific SCIF, at least five working days prior to their arrival.

c. Each Center SSO or SSR is responsible for verification and validation of all persons entering SCIFs.

3.19.6 Use of Scattered Castles. ICD 704, mandates the recognition, use, and reciprocity of the Scattered Castles database to validate clearance/access levels.

3.19.7 For eligibility for a Scattered Castles account, an individual will, at a minimum, have the following:

a. TS/SCI access.

b. Valid JWICS account.

c. Valid PKI certificate.

3.19.8 Requests for Scattered Castles access will be submitted through the CCPS to the Agency SSO.

3.19.9 Only the Agency SSO may grant access to Scattered Castles.

3.19.10 Misuse of the Scattered Castles database will result in immediate revocation of access.

3.20 Training

3.20.1 Annual refresher training is mandatory for all SCI-indoctrinated individuals.

3.20.2 Center SSOs will provide the required training, which should cover, at a minimum, all security training required by Executive Order or policy, including reinforcing the SCI training provided during the security orientation and indoctrination as well as informing cleared individuals of any changes in security regulations and policies.

3.20.3 Non-compliance with completing the annual training requirement may result in the suspension of an individual's SCI access.

3.20.4 Refresher training will be documented in writing for each SCI-indoctrinated individual on the "Certification of Completion of Annual SCI Refresher Training" form or input for retention into NASA's training database. 3.20.5 Training records will be retained for a period of five years.

Chapter 4. Security Education and Training

4.1 General

4.1.1 Security education plays a critical role in the effectiveness of NASA's information security program. This chapter provides an overview of the required security education and training required by Section 5.4 of the E.O. 13526 and 32 CFR pt. 2001 subpt. G.

4.2 Initial Security Education and Training

4.2.1 The CCPS/CCS shall develop, issue, and document initial training. Personnel who have been the subject of a personnel security investigation and granted a security clearance based upon a favorable determination of the investigation results have met the requirements necessary to have access to classified information.

4.2.2 Training is conducted in conjunction with the execution of the most current version of the SF-312. The training should be supplemented with the ISOO SF-312 Briefing Booklet. This booklet provides a brief discussion of the background and purpose of the SF-312; the text of pertinent legislative and executive authorities; a series of questions and answers on its implementation; and a copy of the SF-312.

4.2.3 Clearance holders shall execute the SF-312 by reviewing and signing the form immediately following initial security education training.

4.2.4 All cleared Agency personnel will receive initial training on basic security policies, principles, and practices, as well as criminal, civil and administrative penalties.

4.3 Annual Refresher Security Education and Training

4.3.1 CCPS/CCS will ensure Center clearance holders have completed annual refresher training for employees who create, process, or handle classified information. CCPS/CCS will also reinforce CNSI policies, principles and procedures covered in initial, annual and specialized training periodically throughout the year.

4.3.2 OPS will ensure the annual refresher training remains up-to-date and addresses policies and procedures for properly handling CNSI. The training will also address the identification and handling of other agency-originated information and foreign government information, as well as the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Annual refresher training will be updated periodically to include issues or concerns identified during agency self-inspections.

4.4 Original Classification Training

4.4.1 All OCAs will receive initial training and at least annually, in proper classification and declassification with an emphasis on the avoidance of over-classification as provided in E.O. 13526

and 32 CFR § 2001.71. At a minimum, the training will cover:

- a. Classification standards.
- b. Classification levels.
- c. Classification authority.
- d. Classification categories.
- e. Duration of classification.
- f. Identification and markings.
- g. Classification prohibitions and limitations.
- h. Sanctions.
- i. Classification challenges.
- j. Security classification guides.
- k. Information sharing.

4.4.2 OCAs who do not receive such mandatory training will have their classification authority suspended by the SAO until such training is completed. A waiver may be granted by the SAO if an individual is unable to receive training due to unavoidable circumstances. Whenever a waiver is granted, the individual will receive training as soon as practicable. The Administrator and the Deputy Administrator will coordinate with the SAO before using their authority to suspend or grant a waiver for training so that appropriate records are maintained.

4.5 Derivative Classifier Training

4.5.1 The CCPS/CCS will develop, issue, and document derivative classification training in accordance with E.O. 13526 and 32 CFR § 2001.71 for new individuals authorized to process derivative classification actions and procedures. CCPS/CCS may use DSS or ISOO training to meet this requirement. Prior to performing derivative classification activities, authorized individuals will receive training in the proper application of the derivative classification principles of E.O. 13526 and at least once every 2 years thereafter. At a minimum, this training should include:

- a. Principles of derivative classification.
- b. Classification levels.
- c. Duration of classification.
- d. Identification and markings.
- e. Avoidance of over-classification.
- f. Prohibitions and limitations of classification.
- g. Sanctions.
- h. Classification challenges.

i. Classification guides.

j. Information sharing.

4.5.2 The annual training for clearance holders issued by OPS is considered refresher training for Derivative classifiers. Derivative classifiers who do not receive this training at least once every 2 years will have their authority to apply derivative classification markings suspended by the SAO until the training is completed. A waiver may be granted by the SAO if an individual is unable to receive the training due to unavoidable circumstances. Whenever a waiver is granted, the individual is to receive training as soon as practicable. The Administrator and Deputy Administrator have the authority to suspend and waive training, but the SAO has the primary responsibility for this function.

4.5.3 Derivative classifiers will also be advised of the requirements for marking in the electronic environment (to include email). Documents and emails created in the electronic environment are subject to the same marking requirements as hard copy CNSI as described in Section 1.6 of the E.O. 13526 and 32 CFR § 2001.21. The ISOO Marking Booklet should be used as a supplemental training tool.

4.6 Other Specialized Security Education and Training

4.6.1 Classification management officers, security managers, and security specialists. CCPS/CCS shall ensure that personnel whose duties significantly involve the creation or handling of classified information receive more detailed or additional training immediately after assumption of duties that require other specialized training. Individuals designated to perform these duties will receive specialized training on the specific requirements of each position.

4.6.2 Department of Energy Clearance Holders. Upon approval in NAMS, the clearance holder shall be required to take training in SATERN. Refresher training for DOE clearance holders is once every 2 years thereafter.

4.6.3 Declassification Authorities. After a CCPS/CCS designates an individual as DCA, they shall ensure that the DCA attends the required NASA OPS Declassification Authority Training and the DOE Historical RD/FRD Records Reviewer Training within one year as per 2.11.2a. of this NPR. Additionally, certified DCAs are required to attend refresher training every 3 years provided by NASA OPS.

4.6.4 Safe Custodians. The CCPS/CCS shall ensure personnel designated as a safe custodian or alternate safe custodians be briefed on their responsibilities related to the handling, storage, and protection of CNSI. Additionally, custodians are briefed on the importance of protecting safe combinations, not writing them down or sharing with anyone other than approved personnel. Custodians will receive refresher briefings on their responsibilities annually.

4.6.5 Courier Briefings. The CCPS/CCS shall ensure personnel designated as couriers be briefed that classified material remains in their physical possession at all times, taken from point A to point B in the most direct manner (i.e., not in checked baggage, left unattended in a hotel room or vehicles, safeguarded in hotel safety boxes, or taken to bars, dining, or places of entertainment) and protected from opening, examination, or inspection. Furthermore, designated couriers will be briefed and acknowledge that their authorization to courier CNSI is only valid within the U.S. and its Territories. Couriers will be briefed on their responsibilities annually.

4.6.6 Classified Information Technology Briefings.

- a. NASA OPS shall ensure personnel granted system access and privileges to process, store and transmit classified on certified and accredited NASA National Security Systems receive an initial User Briefing regarding their responsibilities.
- b. Users will also receive initial training of the classification marking tool used when sending classified emails on certified and accredited NASA National Security Systems.

4.6.7 Inadvertent Exposure Briefings.

- a. The CCPS/CCS shall perform an inadvertent exposure briefing. This type of briefing should be performed when an individual is inadvertently exposed to classified information. A document detailing the individual's name, date of exposure, date of signature, signature and a statement that the individual understands their responsibility to not further distribute or discuss the classified information that was inadvertently disclosed will be created. This can occur when a non-cleared person is exposed to classified information or when a cleared person is exposed to classified information at a level higher than what they are briefed for.
- b. An inadvertent exposure briefing can also be directed at the direction of the Director, Security Management Division.

4.7 Termination Briefings

4.7.1 Except in extraordinary circumstances, each employee who is granted access to classified information and who leaves the service of NASA or no longer requires access to classified information will receive a termination briefing. Additionally, each employee whose clearance is withdrawn or revoked will receive such a briefing. At a minimum, termination briefings inform each employee of their continuing responsibility not to disclose any classified information to which the employee had access and the potential penalties for non-compliance, and the obligation to return to the appropriate agency official all classified documents and materials in the employee's possession.

Chapter 5. Industrial Security

5.1 General

5.1.1 This chapter provides procedural requirements for implementation of the industrial security program in accordance with E.O. 12829, 32 CFR pt. 2004, and DoD 5220.22.

5.1.2 The NASA NISP ensures the proper protection of classified information when released to current, prospective, or former contractors, licensees, or grantees of NASA. The Agency meets the requirements associated with regulations, classified contract administration rules and requirements, and the processing and control of classified visits for cleared Government and contractor employees involved in its programs/projects.

5.1.3 The SAO for the NISP is the Associate Administrator for Protective Services.

5.1.4 The processing and control of classified and unclassified visits to a Center in relation to classified contracts and meetings is the responsibility of the CCPS/CCS. See local Center security procedures.

5.2 DoD Support

5.2.1 The Defense Security Service (DSS) will act as the Cognizant Security Agency for the NASA Industrial Security Program. DSS serves as the Executive Agent for inspecting and monitoring the contractors, licensees, and grantees who require access to, or who (will) store classified information; and for determining the eligibility for access to CNSI of contractors, licensees, and grantees and their respective employees.

5.2.2 Contractors support a NASA classified contract are required to possess or be eligible to possess a Facility Security Clearance (FCL) at a classification level equal to or greater than the work to be performed. If the prime contractor does not possess a valid FCL or possess the proper classification level required for contract performance, the CCPS/CCS may sponsor the contractor for an FCL at the required FCL level through DSS. The contractor will possess an active Commercial and Government Entity code (CAGE) code, receive/abide by the security guidelines of a NASA issued DD Form 254, and complete other applicable industrial security forms that require compliance with the NISPOM for industrial security matters. A DD Form 254 will not be issued to any Foreign contractors, foreign governments or North Atlantic Treaty Organization (NATO) activities which require access to classified information..

5.2.3 NASA holds authority to inspect contractor operations approved to access and/or safeguard NASA classified information. Authority details are located on contract specific DD Form 254 as well as contract specifications.

5.3 NISP Responsibilities

5.3.1 The SAO for the NISP shall:

a. Identify the Senior Official for insider threat to ISOO to facilitate information sharing.

- b. Enter into and maintain an agreement with the Office of the Secretary of Defense, DSS.
- c. Submit cost reports to ISOO.
- d. Ensure agency personnel who implement the NISP receive appropriate education and training.
- e. Ensure that adverse information and insider threat activity pertaining to contractor, licensee, or grantee employees having access to classified information are reported to the CSA, DSS.

5.3.2 NASA program or project management personnel contemplating offers or estimates for a classified contract, negotiating or awarding a classified contract, or bearing responsibility for the performance of a classified contract shall:

- a. Ensure the CCPS/CCS is fully engaged in supporting the development of security requirements for the contract.
- b. Provide adequate resources to the CCPS/CCS for program security oversight, as required.
- c. Ensure the contractor's designated facility security officer (FSO) passes a Visit Authorization Letter (VAL) to the CCPS/CCS. At a minimum, a new VAL will be passed on a yearly basis, pursuant to the NISPOM, or when a contractor personnel are added or deleted from the contract.

5.3.3 The Procurement Officer of each Center is responsible for the following:

- a. Ensuring that the request for proposals or offers includes a statement that the contractor or prospective contractor will or will not require access to classified information and will or will not generate classified information in the performance of such contract. If the contract involves access to classified information or the generation of classified information, a letter requiring each contractor to comply with the National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M as required, will be attached to the material submitted to the individual negotiating the contract.
- b. Ensuring that each classified contract contains the standard security requirements clauses prescribed by FAR subpt. 4.4 and NASA FAR Supplement subpt. 1804.4.
- c. Ensuring that a DD Form 254 is included in the solicitation phase and that the Center CCPS/CCS is involved in the completion of the form.
- d. Ensuring that any proposed deviation in this standard security provision (elimination, addition, or substitution) is forwarded to the Office of Procurement for approval by the Assistant Administrator for Procurement, with concurrence by the AA for Protective Services and the NASA Office of General Counsel (OGC).

5.3.4 The CCPS/CCS shall:

- a. Implement the Government Contracting Agency responsibilities of the NISP for industrial security services of contractors on NASA Centers and facilities, excluding personnel security clearances.
- (1) Ensure that NASA recommendations affecting the contractor's security program are made primarily through the cognizant security office DSS for the contractor concerned, since DSS is primarily responsible for ensuring that the contractor complies with all security recommendations. When it becomes apparent that full and satisfactory action on a specific NASA recommendation has not been taken by the cognizant security office or by the contractor, a detailed report of the

circumstances will be forwarded to the AA for Protective Services for appropriate action with a copy to the contracting officer.

b. Process and control classified and unclassified visits to a Center in relation to classified contracts as covered in written local security procedures tailored to that Center.

c. Ensure contractors operating under a DD Form 254 provide the appropriate “Classified Visit” documentation, pursuant to the NISPOM, on all “cleared” contractor personnel working under the DD Form 254 and ensure updates are provided on an as needed basis. Classified visit requests are mandatory for all NASA Classified Contracts.

d. Coordinate with the contracting officer and contracting officer’s technical representative, to develop local written security procedures to ensure that the following requirements are met:

(1) The NASA contracting officer has the responsibility to include the DD 254 in the requests for proposal (RFP) and contracts. The Center Security Office has the responsibility for generating the DD-254 and signing the document. Center Security reviews each RFP and/or contract to fully understand the requirements and implications of the procurement action with regard to security.

(2) In item 12 of the DD Form 254, delete the words: “To the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review in accordance with the Industrial Security Manual,” and insert the words: “To the Office of Communications, National Aeronautics and Space Administration, Washington, DC 20546, for review.”

(3) In the case of prime contracts, also specify “the Office of Communications Public Information Office of the NASA contracting Center” in item 12 to indicate that proposed publicity releases will be submitted through that office to the Office of Communications.

(4) In the case of subcontracts, the publicity office of the prime contractor will be specified, in addition to the Office of Communications Public Information Office of the NASA Contracting Center, to indicate that proposed publicity releases will be submitted through those two offices to the NASA Office of Communications.

5.3.5 All changes to a contractor’s security program that may affect the cost, performance, or delivery of a contract are submitted to the contracting officer and, where appropriate, contract modifications will be processed accordingly.

5.4 Suspension, Revocation, and Denial of Access to Classified Information

5.4.1 Center Security Offices may find it necessary to take action to suspend, or deny a NASA contract employee’s access to CNSI or, in coordination with the NASA contracting officer, to suspend operation of the entire contract. To ensure uniformity and consistency, the following applies:

a. In the rare cases NASA has granted a contractor’s clearance, only the AA for Protective Services or designee may deny or revoke a cleared contractor’s access to classified information.

b. The AA for Protective Services, Center Director, CCPS/CCS, or the OPS Security Management Division Director shall suspend a contractor’s access for cause.

5.4.2 Each action will be fully documented. Information developed during the security inquiry will not be shared with the contracting officer or contractor management while the inquiry is ongoing. The Office of Protective Service/OPS Security Management Division Director or CCPS/CCS may override this principle, if in their judgment the information suggests that the subject poses an immediate and serious threat to the health or safety of other individuals, is a threat to a critical mission, or may otherwise be ineligible for continued access to classified information.

5.4.3 Center security officials shall ensure coordination is effected with the local or regional Industrial Security investigative organization (OPM and DSS) to obtain direction and to ensure information is provided to enable them to properly adjudicate for continued clearance eligibility.

5.4.4 During the investigative and adjudicative process, all reasonable efforts will be pursued to fully develop potential issue information, as well as potentially favorable or mitigating information.

5.4.5 The CCPS/CCS shall propose denials and revocations of contractor access to the AA for Protective Services. The AA for Protective Services will make final denial or revocation determinations after consultation with the NASA Central Adjudication Facility and the OGC.

5.4.6 Subjects of adjudication will be allowed to review and refute any information developed during the investigation process that makes him or her ineligible for access to NASA CNSI, unless release of that information jeopardizes national security.

5.5 Requirements of DD Form 254

5.5.1 The CCPS/CCS shall also include a contract security classification specification, DD Form 254, with each contract or agreement and solicitation that requires access to classified information. The DD Form 254 identifies the specific elements of classified information involved in each phase of the contract or agreement life-cycle, such as:

- a. Level of classification;
- b. Where the entity will access or store the classified information, and any requirements or limitations on transmitting classified information outside the entity;
- c. Any special accesses;
- d. Any classification guides or other guidance the entity needs to perform during that phase of the contract or agreement;
- e. Any authorization to disclose information about the classified contract or agreement; and
- f. GCA personnel responsible for interpreting and applying the contract security specifications (or equivalent guidance).

5.5.2 The CCPS/CCS shall revise the contract security classification specification throughout the contract or agreement life-cycle as security requirements change.

- a. Classification guidance is the exclusive responsibility of the CCPS/CCS. The CCPS/CCS prepares classification guidance in accordance with 32 CFR § 2001.15, and provides appropriate security classification and declassification guidance to entities.
- b. The CCPS/CCS responds to requests for clarification and classification challenges.

c. Instructions upon contract or agreement termination.

(1) The CCPS/CCS provides instructions to the contractor, licensee, or grantee for returning or disposing of classified information upon contract or agreement termination or when an entity no longer has a legitimate need to retain or possess classified information.

(2) The CCPS/CCS also determines whether the contractor, licensee, or grantee may retain classified information for particular purposes after the contract or agreement terminates, and if so, provides written authorization to the entity along with any instructions or limitations (such as which information, for how long, etc).

5.5.3 Each approved DD Form 254, Contract Security Classification Specification, or other written notification, issued in lieu thereof, is reviewed at least annually by CCPS/CCS with the assistance of the procurement office.

5.5.4 The individual(s) responsible for this review is identified by the CCPS/CCS in local written security procedures.

5.5.5 When a change is made in a security classification specification pertaining to a prime contract, that change will be reflected in all applicable DD Form 254s or other classification documents pertaining to subcontractors.

Appendix A. Definitions

Access. The ability or opportunity to gain knowledge of classified information.

Adjudication. A fair and logical Agency determination, based upon established adjudicative guidelines and sufficient investigative information, as to whether or not an individual's access to classified information, suitability for employment with the U.S. Government, or access to NASA facilities, information, or IT resources, is in the best interest of national security or efficiency of the Government.

Authorized holder. Anyone who satisfies the conditions for access to classified information in accordance with section 4.1 (a) in E.O. 13526.

Automatic declassification. The declassification of information based solely upon the occurrence of a specific date or event as determined by the original classification authority or the expiration of a maximum timeframe for duration of classification established under E.O. 13526.

Center Chief of Protective Services/Center Chief of Security (CCPS/CCS). The senior Center security official responsible for technical management of the Center security program.

Certification. A formal process used by the Certifying Official to ensure that an individual has met all established training requirements necessary to perform their security responsibilities.

Central Adjudication Facility (CAF). Facility established at the Security Management Division-level which is responsible for adjudicating all requests for clearances to access CNSI.

Classification. The act or process by which information is determined to be classified information.

Classification guidance. Any instruction or source that prescribes the classification of specific information.

Classification Guide. A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that is classified and establishes the level and duration of classification for each such element.

Classified Material. Any physical object of which requires protection against unauthorized disclosure and is marked to indicate its classified status including objects that contain recorded or embody CNSI that is discerned by the study, analysis, observation, or other use of the object itself.

Classified National Security Information (CNSI). Information, material, equipment, or other artifacts that is protected against unauthorized disclosure in accordance with E.O. 13526 and is marked to indicate its classified status when in documentary form.

Closed Area. An area in which security measures are taken to safeguard classified material where entry to the area alone provides visible or audible access to classified material.

Collateral Classified. All CNSI, excluding information in the SCI or SAP information category.

Communications Security (COMSEC). Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes crypto security, transmission security, emission security, and physical security of COMSEC material.

Compilation. An aggregation of pre-existing unclassified items of information.

Compromise. The improper or unauthorized disclosure of or access to classified information.

Damage. Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

Declassification. The authorized change in the status of information from classified information to unclassified information.

Declassification Authority (DCA). An official delegated declassification authority in writing by the Agency head or the SAO.

Declassification Guide. Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that remain classified.

Denial. The adjudication that an individual's initial access to classified information would pose a risk to national security, after review procedures set forth in E.O. 13526 have been exercised.

Derivative classification. The incorporation, paraphrasing, restating, or generation of a new form of information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Document. Any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

Downgrading. A determination by a declassification authority that information classified and safeguarded at a specified level is classified and safeguarded at a lower level.

Escort. A NASA civil service employee or contractor responsible for the management of a visitor's movements and/or accesses implemented through the constant presence and monitoring of the visitor by appropriately designated and properly trained U.S. Government or approved contractor personnel. Training includes the purpose of the visit, where the individual may access the Center, where the individual may go, whom the individual is to meet, and authorized topics of discussion.

File Series. File units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

Foreign Government Information.

Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence.

Information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, an international organization of governments or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence.

information received and treated as foreign government information under the terms of a predecessor order.

Foreign National. For the purpose of general security protection, considerations of national security, and access accountability: Any person who is not a citizen of the United States. Includes lawful permanent resident (i.e., holders of green cards) or persons admitted with refugee asylee status to the United States.

Formerly Restricted Data (FRD). Defined by 42 U.S.C. § 2011 et seq. as classified information which has been removed from the RD category after DOE and the DOD have jointly determined that it relates primarily to the military's utilization of atomic weapons and can be adequately safeguarded as national security information.

Information Security Oversight Office (ISOO). Office established under the Executive Office of the President tasked with policy development and oversight of Federal agency compliance with national-level policy for management of CNSI.

Limited Area. An area in which security measures are taken to safeguard classified material or unclassified property warranting special protection. To prevent unauthorized access to such property, visitors are escorted or other internal restrictions implemented, as determined by the CCPS/CCS.

Mandatory Declassification Review. The review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of E.O. 13526.

NASA Employee. NASA civil service personnel.

National Security. The national defense or foreign relations of the United States.

National Security Position. Positions that have the potential to cause damage to the national security. These positions require access to classified information and are designated by the level of potential damage to the national security:

a. Confidential. Information, the unauthorized disclosure of which reasonably could be expected to cause damage to national security that the Original Classification Authority is able to identify or describe.

b. Secret. Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security that the Original Classification Authority is able to identify or describe.

c. Top Secret. Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security that the OCA is able to identify or describe.

Need-to-Know. A determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Nondisclosure Agreement. SF 312 is a non-disclosure agreement required under E.O. 13526 and 32 CFR pt. 2001 to be signed by employees of the U.S. Federal Government or one of its contractors when they are granted a security clearance for access to classified information. The form is issued by the ISOO of the NARA and its title is "Classified Information Nondisclosure Agreement." All persons with authorized access to classified information are required to sign a nondisclosure

agreement as a condition of access. This requirement is reiterated in the executive order on classified national security information. The SF 312 is a contractual agreement between the U.S. Government and you, a cleared employee, in which you agree never to disclose classified information to an unauthorized person. Its primary purpose is to inform you of (1) the trust that is placed in you by providing you access to classified information; (2) your responsibilities to protect that information from unauthorized disclosure; and (3) the consequences that may result from your failure to meet those responsibilities. Additionally, by establishing the nature of this trust, your responsibilities, and the potential consequences of noncompliance in the context of a contractual agreement, if you violate that trust, the United States will be better able to prevent an unauthorized disclosure or to discipline you for such a disclosure by initiating a civil or administrative action.

Original Classification. An initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

Original Classification Authority (OCA). An individual authorized in writing, either by the President, by agency heads, or other senior Government officials designated by the President, to classify information in the first instance.

Page Check. Involves visually sighting each page in a document, verifying its presence against a list of effective pages (if applicable), and ensuring that the page is from the original document. In the absence of a list of effective pages, the document will be examined for continuity.

Lawful Permanent Resident. A non-U.S. citizen legally permitted to reside and work within the United States and issued the Permanent Resident Card (Green Card). Afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the Federal sector (except for specific needs or under temporary appointments per 3 CFR pt. 7 & §7.4), and access to CNSI. Lawful Permanent Residents are not prohibited from accessing export controlled commodities, but will have a work-related need-to-know in order to access. Legal Permanent Residents are considered foreign nationals under immigration laws.

Personally Identifiable Information. Any information about an individual which can be used to distinguish or trace an individual's identity. Some information that is considered to be PII is available in public sources such as telephone books, public websites, university listings, etc. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. In contrast, Protected PII is defined as a social security number as a stand-alone, or an individual's first name or first initial and last name in combination with any one or more types of the following information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, etc. This information may be in the form of paper, electronic or any other media format.

Records. The records of an agency and Presidential papers or records, as those terms are defined in 44 U.S.C. § 2905, § 3101, and § 3102, including those created or maintained by a Government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant. Records having permanent historical value include Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with 44 U.S.C. §§ 2905, 3101, and 3102.

Restricted Area. An area in which security measures are taken to safeguard and control access to

property and hazardous materials or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. All facilities designated as critical infrastructure or key resource are “Restricted” areas (as a minimum designation).

Restricted Data (RD). Defined by the 42 U.S.C. § 2011 et seq. as all data concerning design, manufacture, or utilization of atomic weapons, production of special nuclear material, and use of Special Nuclear Material in the production of energy.

Safeguarding. Measures and controls that are prescribed to protect classified information.

Security Classification Guide. The written direction issued or approved by a Top Secret/OCA that identifies the information or material to be protected from unauthorized disclosure and specifies the level and duration of classification assigned or assignable to such information or material.

Security Clearance. A designation identifying an individual's highest level of allowable access to classified information based upon a positive adjudication that the individual does not pose a risk to national security.

Security Management Division Director. Official assigned to the OPS who is responsible for Agency management of personnel security, physical security, industrial security, electronic physical access control systems, and identity, credential and access management.

Security Violation. A security violation is potential or actual compromise.

Security Infraction. A security infraction will NOT result in compromise, usually administrative in nature.

Self-inspection. The internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under E.O. 13526 and its implementing directives.

Senior Agency Official (SAO). The official designated by the agency head under section 5.4 (d) of E.O. 13526 to direct and administer the agency’s program under which information is classified, safeguarded, and declassified.

Sensitive Compartmented Information (SCI). Classification level denoting information, generally intelligence related, requiring security clearances and physical/procedural security measures above those established for collateral classified information or SAP information.

Source Document. An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Special Access Program (SAP). Any program established and approved under E.O. 13526 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

Suspension. The temporary removal of an individual’s access to classified information, pending the completion of an investigation and final adjudication.

Systematic Declassification Review. The review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with 44 U.S.C. § 2905, § 3101, and § 3102.

Unauthorized Disclosure (E.O. 13526). A communication or physical transfer of classified

information to a recipient who does not have the appropriate credentials for access.

Waiver. The approved continuance of a condition authorized by the AA for Protective Services that varies from a requirement and implements risk management on the designated vulnerability.

Appendix B. Acronyms

AA	Assistant Administrator
APO	Army Post Office
CAF	Central Adjudication Facility
CAM	COMSEC Account Manager
CAGE CODE	Commercial and Government Entity Code
CCPS	Center Chief of Protective Services
CCS	Center Chief of Security
CFR	Code of Federal Regulations
CMCO	Classified Material Control Officer
CNSI	Classified National Security Information
CNSS	Committee on National Security Systems
CNSSI	Classified National Security System Instruction
COMSEC	Communications Security
COR	Central Office of Record
CSA	Cognizant Security Agency
CSOP	Central Office of Record Standard Operating Procedures
DCA	Declassification Authority
DCP	Document Control Points
DCS	Defense Courier Service
DCSO	Document Control Station Official
DOD	Department of Defense
DOE	Department of Energy
DSS	Defense Security Service
EAR	Export Administration Regulation
FedEx	Federal Express
FGI	Foreign Government Information
FPO	Fleet Post Office
FRD	Formerly Restricted Data
IPA	Intergovernmental Personnel Act

IS	Information Systems
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
ITAR	International Traffic in Arms Regulation
LAA	Limited Access Authorization
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NISPOM	National Industrial Security Program Operating Manual
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NSA	National Security Agency
NSTISSI	National Security Telecommunications Information Systems Security Instruction
PII	Personally Identifiable Information
OCA	Original Classification Authority
OGC	Office of General Counsel
OPM	Office of Personnel Management
OPS	Office of Protective Services
RD	Restricted Data
SAO	Senior Agency Official
SAP	Special Access Program
SAPSG	Special Access Program Security Guide
SCG	Security Classification Guides
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCP	Security Control Point
SF	Standard Form
SME	Subject Matter Expert
SSO	Special Security Officer

TSCO	Top Secret Control Officer
UCNI	Unclassified Controlled Nuclear Information
U.S.C.	United States Code
USPS	United States Postal Service

Appendix C. Derivative Classification in Electronic Media

C.1 How to determine if an Electronic Record is a Derivative Classification Action:

C.1.1 E-mail: If a classified e-mail is disseminated and no additional classified information is added in the replies or forwards, then only the first classified e-mail should be counted. The replies and forwards that do include additional classified information should be counted in addition to the original classified e-mail. Do not count unclassified e-mails that are created on a system that is certified to handle classified information. If the e-mail is merely a transmittal vehicle for a classified attachment and contains no classified information itself, then do not count the e-mail. Only count the classified attachment if it was originated by your office.

C.1.2 Web pages: Each web page containing classified information that is created during the reporting period should be counted only once regardless of how many times it was modified or updated. The count should be conducted by the agency or command that hosts the web page.

C.1.3 Blogs: Every individual blog entry that constitutes a classification action should be counted. The count should be conducted by the agency or command hosting the blog.

C.1.4 Wiki articles: Each wiki article containing classified information that is created during the reporting period should be counted, and counted only once, regardless of how many times it is modified or updated by other users. The count should be conducted by the agency or command hosting the wiki.

C.1.5 Instant messages: Instant messages should not be counted.

C.2 Table A provides examples of how to count decisions in both the paper environment and the electronic environment.

Table A. Decision Counting Examples

Paper environment	Electronic environment	How to count
A report contains classified information derived from a classified source and is photocopied and distributed to 30 recipients.	An e-mail contains classified information derived from a classified source and is disseminated to 20 recipients, and then forwarded on to 10 more recipients.	Count as one classification decision. Do not count as 30 or 31 classification decisions.
An unclassified internal memo is drafted in response to a classified Inspector General (IG) report. The IG report will be distributed as an attachment to the unclassified internal memo.	An unclassified transmittal E-mail is drafted in response to a classified IG report. The IG report will be distributed as an electronic attachment to the unclassified e-mail.	Do not count as a classification decision. A classification decision was already counted at the creation of the classified IG report. The e-mail will be protected as classified (classified transmittal) but does not warrant a classification count.

Appendix D. References

D.1 Procedures, 50 U.S.C. § 435.

D.2 Security Requirements for Government Employees, as amended E.O. 10450.

D.3 Administrative Personnel Suitability Determination, 5 CFR § 731.202.

D.4 Personal Identity Verification (PIV) of Contractor Personnel, 48 CFR Federal Acquisition Regulation Clauses 52.204-9.

D.5 National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4004, Annex B.

D.6 NPD 1600.2, NASA Security Policy.

D.7 NPR 1382.1, NASA Privacy Procedural Requirements.

D.8 NASA Declassification Management Plan.

D.9 NASA Special Access Program Security Guide (SAPSG).

D.10 NF 1801, Declassification Review Report.